LONGSHINE®

User Manual

Model No. LCS-WRM-3214

ADSL2/2+ 4 Port Wireless Router

For Annex A/B

Version 1.0
May.2006

Table of Contents

Specification *4*

Package Contents *6*

Hardware Connecting *7*

LED Indicators *7*

General Setting *8*

Advanced Setup *12*

Setup 12

LAN Setup 12

LAN Configuration 12

Ethernet Switch 14

WAN Setup 15

Two Step PVC 15

New Connection 16

PPPoE Settings 19

PPPoA Settings 21

Static Settings 23

DHCP Settings 24

Bridge Settings 25

CLIP Settings 26

Modem 27

ADVANCED 28

UPnP 28

SNTP 29

SNMP 30

TR-069 31

Port Forwarding 32

DMZ 33

Custom Port Forwarding 34

IP Filter 35

Custom IP Filters 35

LAN Clients 37

LAN Isolation 38

TR-068 WAN Access 39

Bridge Filters 40

Web Filters 42

Dynamic DNS Client 43

IGMP Proxy 44
Static Routing 45
Dynamic Routing 46
Policy Routing 48
Ingress 50
Egress 51
Shaper 52
Web Access Control 53
Web Access Control 53
SSH Access Control 54
WIRELESS 55
Setup 55
Configuration 56
Multiple SSID 57
Security 58
Management 59
WDS 60
TOOLS 65
System Commands 65
Remote Log 66
User Management 67
Update Gateway 68
Ping Test 69
Modem Test 70
STATUS 71
Network Statistics 71
Connection Status 73
DDNS Update Status 73
DHCP Clients 74
Modem Status 74
Product Information 75
System Log 75
WDS Report 76
HELP 77
Firewall Help 77
Bridge Filter Help 77
LAN Clients 78
LAN Group Configuration 78
PPP Connection 79
UPnP Help 79

RIP Help 80
QoS Help 80
Troubleshooting 81
Appendix 88

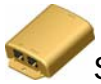
Specification

Line Connection	• RJ-11(2 wires) , RJ-45 (4 port)
ADSL Features	• DMT modulation and demodulation • Tone detection for low power mode • ITU 992.1 (G.dmt) Annex A, B • ITU 992.2 (G.lite) • ITU 992.3 ADSL2 (G.dmt.bis) • ITU 992.5 ADSL2+ • ANSI T1.413 Issue 2
Full-rate adaptive modem	• Maximum downstream rate of 24 Mbps (ADSL2+) • Maximum upstream rate of 1 Mbps
G.lite adaptive modem	• Maximum downstream rate of 1.5 Mbps • Maximum upstream rate of 512 Kbps
WAN Mode Support	• PPP over ATM (RFC 2364) • PPP over Ethernet (RFC 2516)
LAN Mode Support	• Bridged/routed Ethernet over ATM (RFC 2684/1483) • Classical IP over ATM (RFC 1577) and PPP over Ethernet (RFC 2516)
Bridge Mode Support	• Ethernet to ADSL self-learning Transparent Bridging (IEEE 802.1D) • Supports up to 128 MAC learning addresses
Router Mode Support	• IP routing-RIPv2 (backward compatible with RIPv1) • Static routing • DHCP (Dynamic Host Configuration Protocol) Server and Client • NAPT (Network Address and Port Translation) • NAT (Network Address Translation) • ICMP (Internet Control Message Protocol) • Secure HTTP server (HTTPS) • IGMP (Internet Group Management Protocol)
802.11g Wireless Access Point	• 54Mbps Access Point for wireless connectivity • Interoperable with IEEE 802.11g (PBCC & OFDM Modulation • Technology supports) 2.4GHz compliant equipment • Supports full mobility and seamless roaming from cell to cell • Support Ad hoc and Infrastructure mode • Support AP client architecture • Support WEP (64/128/256 bit), WPA/WPA2 • Provides up to 30 users wireless connection • Work range : per node indoors approximately 30m~100m,outdoors (line of sight) 200m~300m depending on data rates • External antenna : one 2dbi detachable antennas with diversity support (Reverse SMA connector)
Ethernet Features	• Four RJ-45 connectors for 10/100 Mbps Ethernet LAN

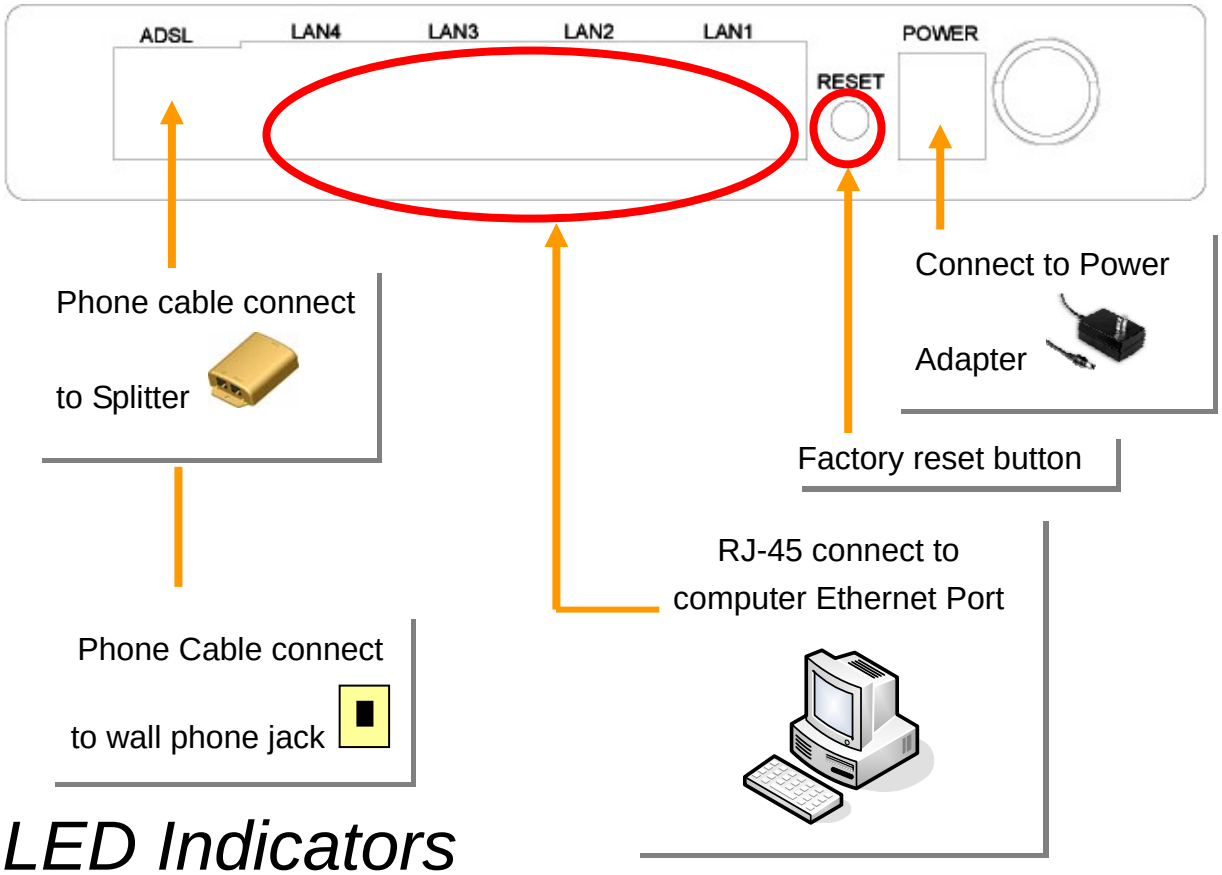
	connection,DMZ function can be set up between them • Complies with IEEE 802.3u specification • Supports Auto-Negotiation • Supports Auto-MDIX, Auto-MDI • Supports IEEE 802.3x Flow control in Full Duplex mode
Certification	• CE,LVD
OS	• WIN 98SE ; WIN 2000；WIN ME；WIN XP
System Requirement	• PII-266 + 32M RAM
Power	• External AC Power • Power ON/OFF switch (option) • Input : 90~120V or 200~240V , 50/60Hz • Output : 12VAC/800mA
LED Indication	• Power , ADSL Link , WLAN , LAN PORT1~4
PCB SIZE	• 134mm×96.5mm
Software Upgrade	• Upgrade by Ethernet Port

Application Diagram

Package Contents

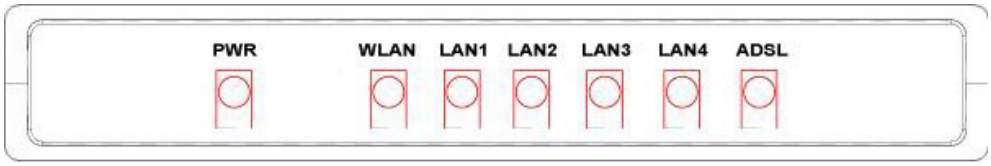
- Longshine ADSL 2/2+ Wireless 4 Port Router
- CD-ROM containing Manual, Quick start Guide
- Ethernet Cable (CAT5 UTP Straight-Through)
- Telephone Cable (RJ11)
- Power Adapter (12VAC 800mA)
- Quick Installation Guide
-  Splitter (Optional)

Hardware Connecting



LED Indicators

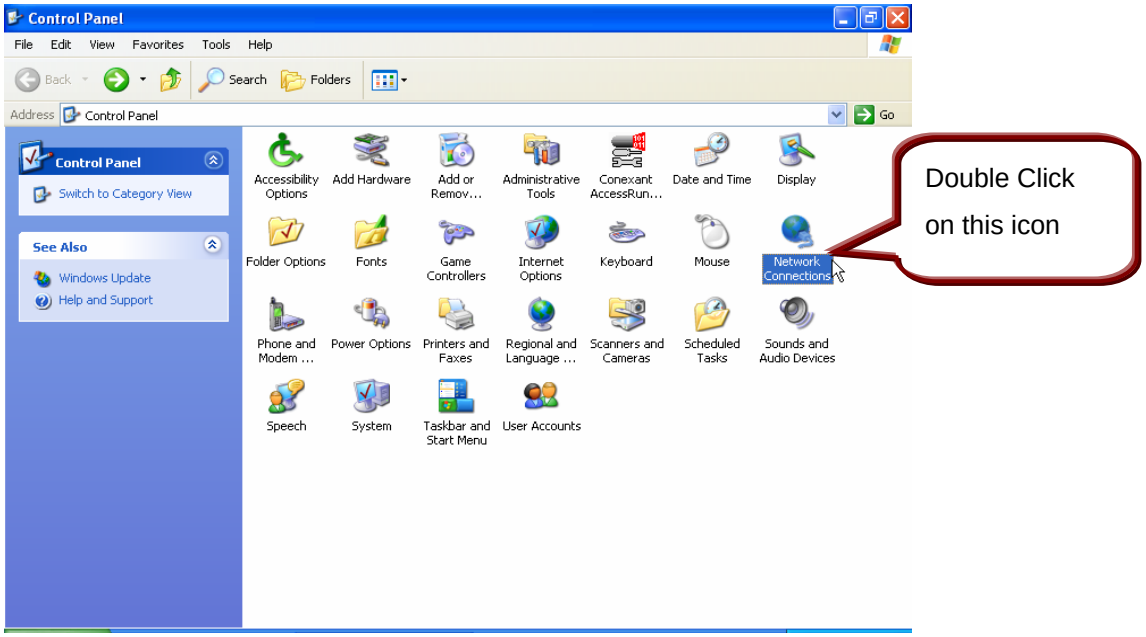
The LED Indicators are located on the front of the unit, they are green in color. The meanings are as follows:



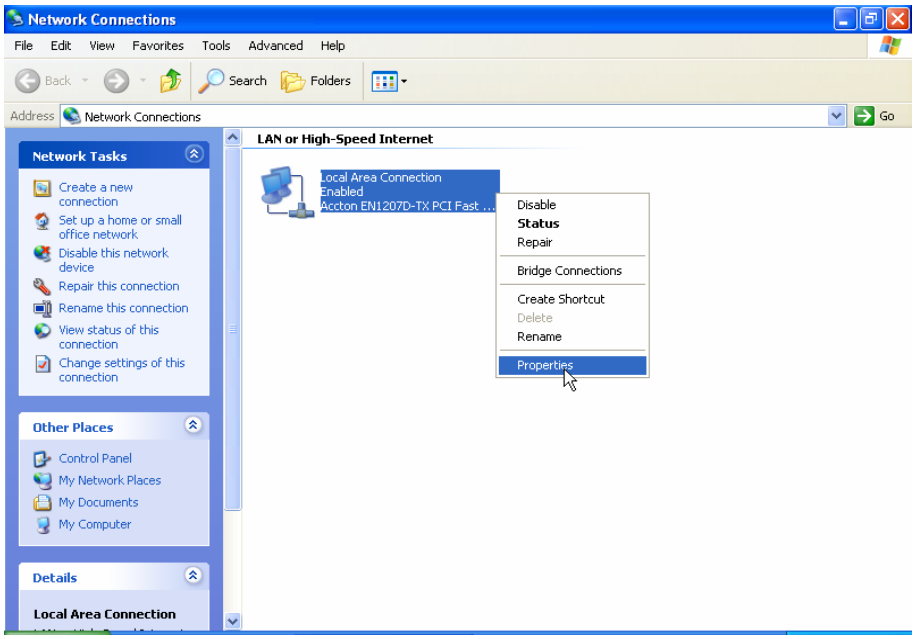
Label	Meaning	Status	Indicates
PWR	Power	On	Power is on
		Off	Power is off
WLAN	Wireless LAN	On	Wireless LAN active.
LAN 1/ LAN 2/ LAN 3/ LAN 4	LAN Link	Flashing	Flashes when data is being sent or received on the LAN connection.
		On	Indicates a link to your LAN or Network card is active.
		Off	Indicates no link to LAN
ADSL	Link	On	A valid ADSL connection.
		Flashing	An active WAN session.
		Off	No ADSL connection.

General Setting

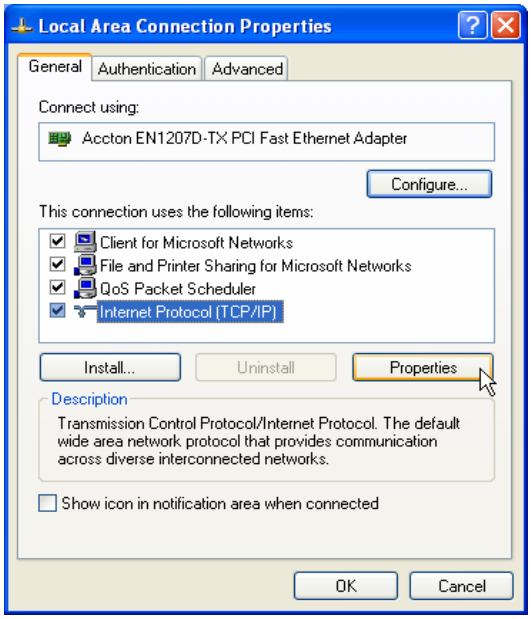
1. Move your cursor as flowing sequence ***Start \ Settings \ Control Panel*** and click ***Control Panel***. Then double-click on the ***Network Connections***



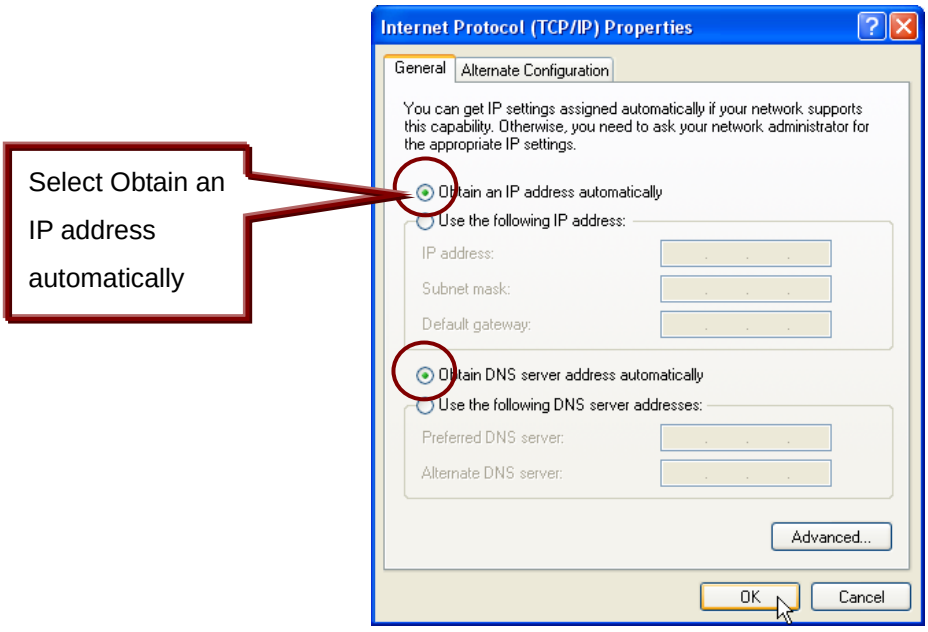
2. In the ***LAN or High-Speed Internet*** window, right-click on icon corresponding to your network interface card (NIC) and select ***Properties***.(This icon may be labeled Local Area Connection).



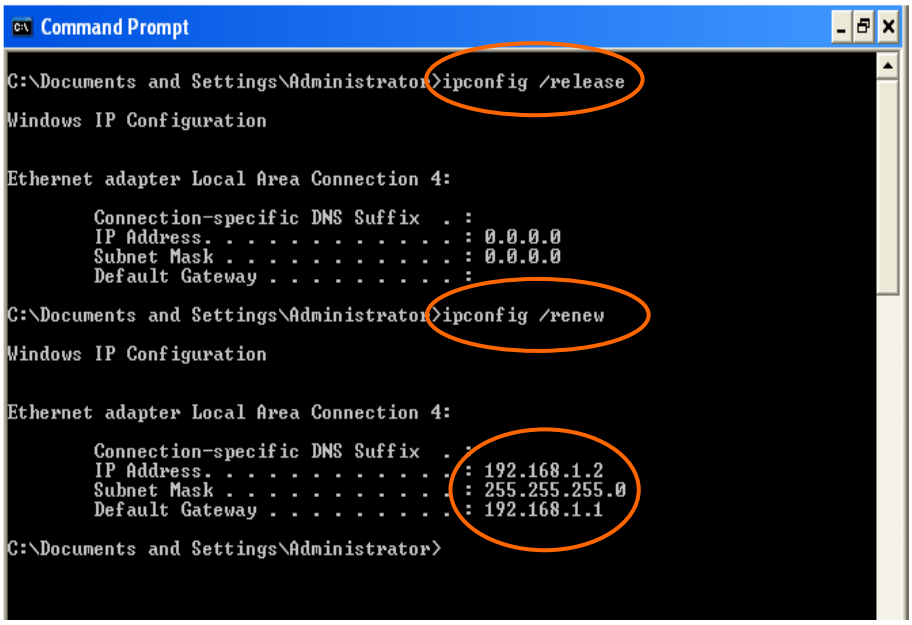
3. In the ***General*** Tab of the ***Local Area Connection Properties*** menu. Highlight ***Internet Protocol (TCP/IP)*** under “This connection uses the following items.” by click on it once. Click on the ***Properties*** button.



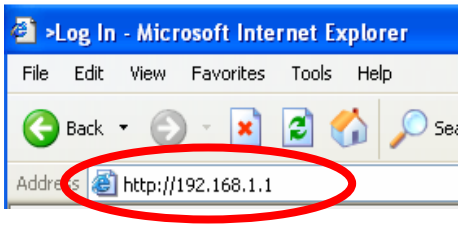
4. Select ***Obtain an IP Address automatically:*** by clicking once in the circle. Click ***OK*** button to confirm and save your changes, and the close the Control Panel.


Select Obtain an IP address automatically
Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

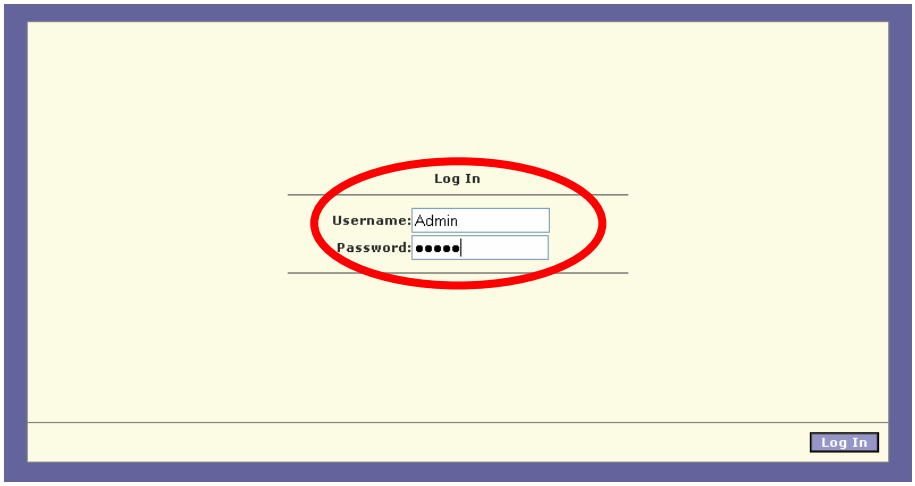
5. Release IP & Renew IP, then Check Default Gateway: ***192.168.1.1***.


Command Prompt
C:\Documents and Settings\Administrator>ipconfig /release
Windows IP Configuration
Ethernet adapter Local Area Connection 4:
Connection-specific DNS Suffix . :
IP Address. . . . . : 0.0.0.0
Subnet Mask . . . . . : 0.0.0.0
Default Gateway . . . . . :
C:\Documents and Settings\Administrator>ipconfig /renew
Windows IP Configuration
Ethernet adapter Local Area Connection 4:
Connection-specific DNS Suffix . :
IP Address. . . . . : 192.168.1.2
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
C:\Documents and Settings\Administrator>

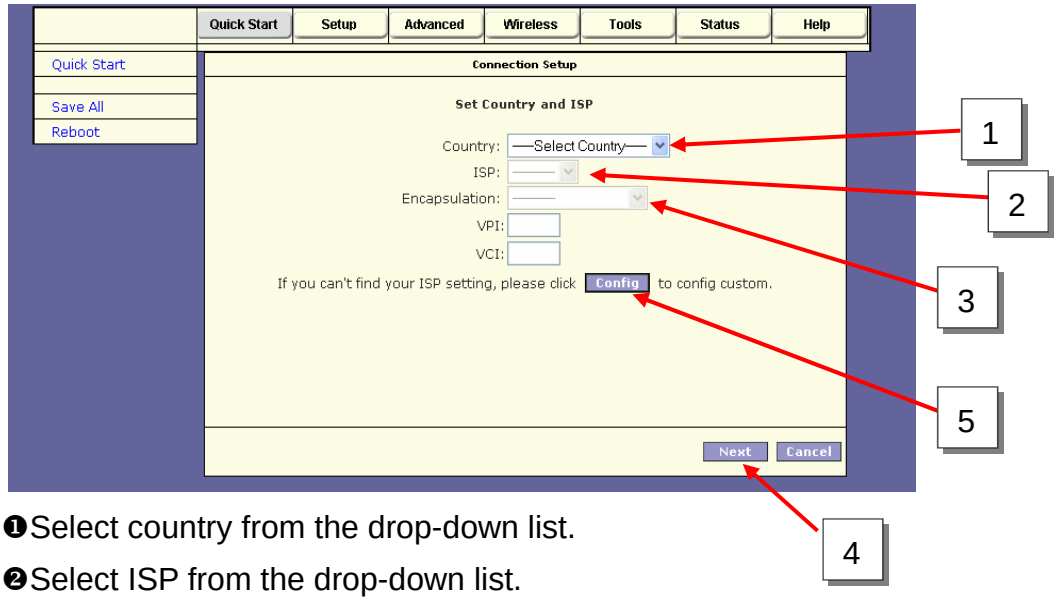
6. Launch your PC web browser and enter the URL: **http://192.168.1.1**



7. Please enter the user name and password as below:
   User name: **Admin**
   Password: **Admin,** And then, click "**Log In**".



8. After Login procedure the **Quick Start** Page will appear.



❶Select country from the drop-down list.

❷Select ISP from the drop-down list.

❸Select Encapsulation from the drop-down list.

❹The VPI and VCI value will automatically set up ok. Then click **Next**.

❺If you can't find your ISP setting, please click **Config**.

Advanced Setup

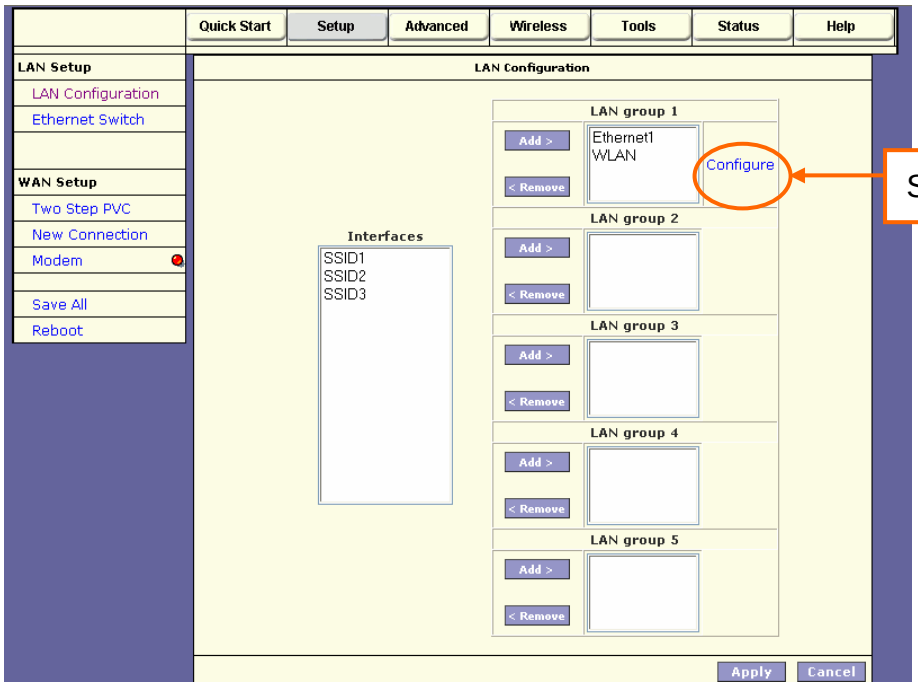
Setup

The Setup section allows you to create new connections, edit existing connections, and configure other basic settings.

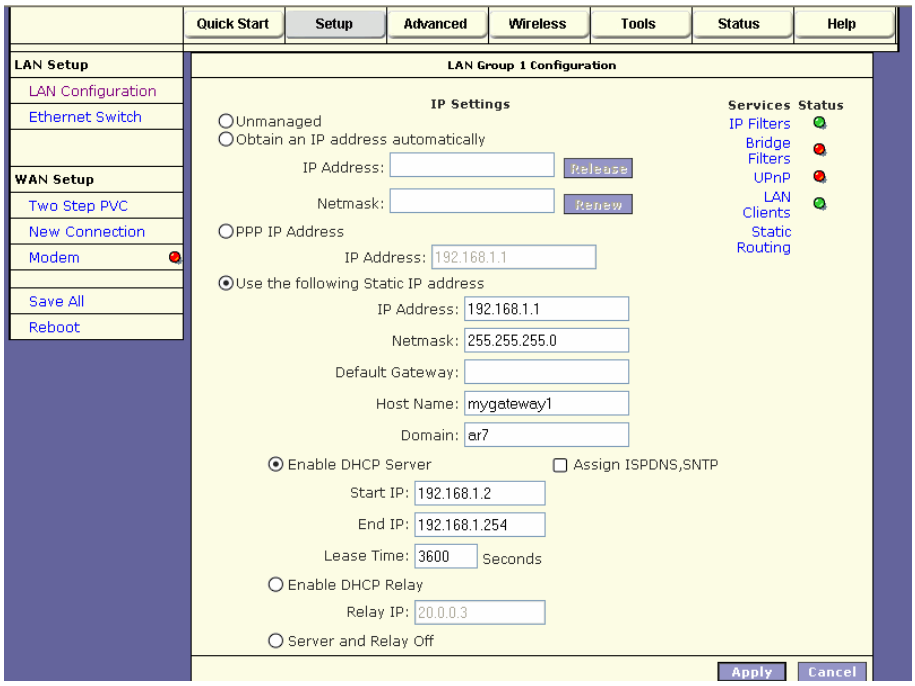
LAN Setup

LAN Configuration

The following is displayed LAN Setup.



Select Configure



IP Address: Private IP address for connecting to a local private network (Default: 192.168.1.1).

Netmask: Netmask for the local private network (Default: 255.255.255.0).

Default Gateway: This field is optional. Enter in the IP address of the router on your network.

Host Name: Required by some ISPs. If the ISP does not provide the Host name, please leave it blank.

Domain Name: www.dynsns.org will provide you with a Domain Name. Enter this name in the “Domain Name” field.

Enable DHCP Server: Enable or Disable DHCP Server.

Start IP: Sets the start IP address of the IP address pool.

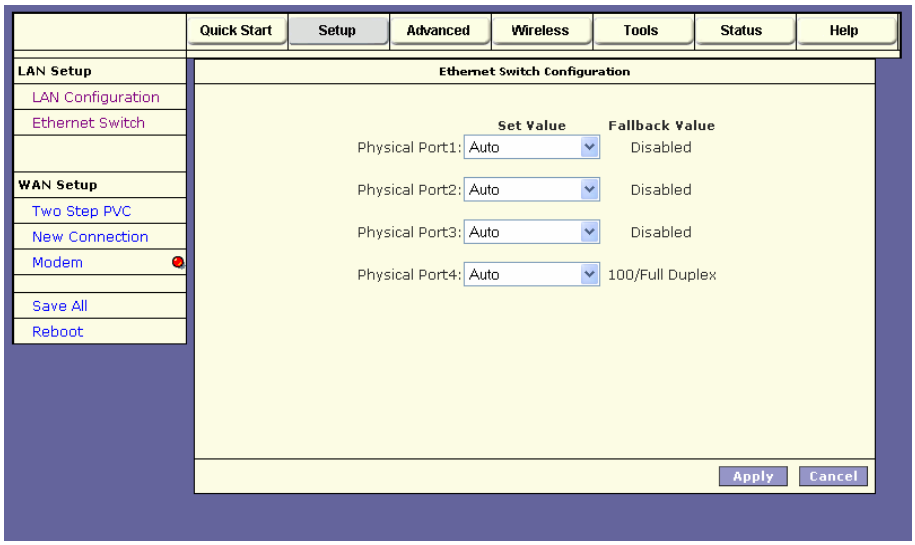
End IP: Sets the end IP address of the IP address pool.

Lease time: The lease time is the amount of time of a network user will be allowed to connect with DHCP server. If all fields are 0, the allocated IP address will be effective forever.

Click ***Apply*** to complete the setup. Click ***Save All*** to save the changes.

Ethernet Switch

This Ethernet Switch Configuration page allows you to set value for data transfer;



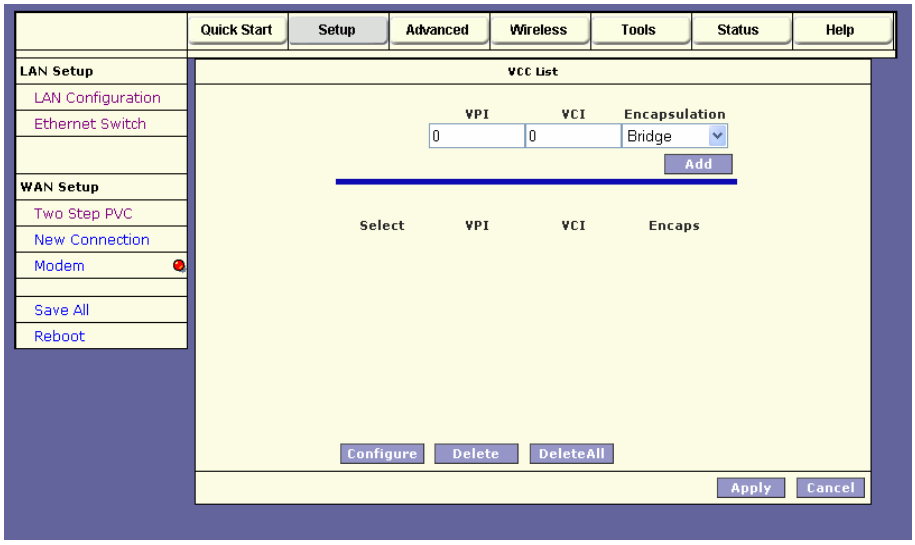
Physical Port: There are five kinds of mode for data transfer (Auto)(10/Half Duplex)(10/Full Duplex)(100/Half Duplex)(100/Full Duplex).

Click ***Apply*** to complete the setup. Click ***Save All*** to save the changes.

WAN Setup

Two Step PVC

The Two-step PVC page is added to support the Remote Management /Clear Embedded Operations Channel (EOC) feature, which is a China MII requirement.

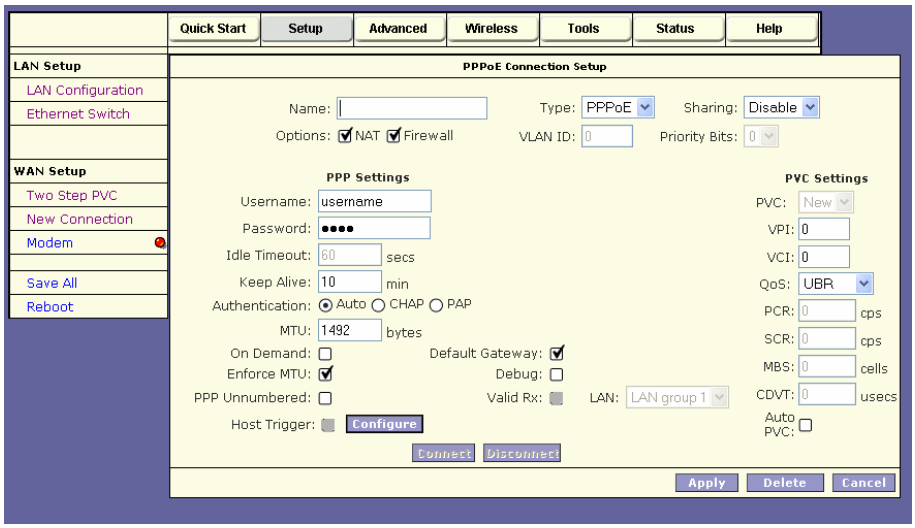


This page allows WAN connections to be created in two steps:

1. Create multiple PVCs with VPI; VCI values, and encapsulation types. The following encapsulation methods are supported:
   PPPoA
   PPPoE
   Router 1483
   Bridge
   Static
   DHCP
   CLIP
2. Create a WAN connection from existing PVC.

New Connection

When working with wide area connections, the first thing you must do is to have the handle of the connection. Once you have the handle for a Connection you must define the PVC and protocol settings for it.



Name: Enter the name of your ISP. This information is for identification purposes only.

Type: There six kinds of method (PPPoE/ PPPoA/ Static/ DHCP/ Bridge/ CLIP).

Encapsulation: Select you encapsulation type. (Supplied by your ISP).

Username: Enter the username provided by your ISP.

Password: Enter the password provided by your ISP.

Idle Timeout: Idle timeout means the router will disconnect after being idle for a preset amount of time. The default is 60 seconds. If you set the time to 0, the link will remain always connected to the ISP.

Keep Alive: When the **On Demand** option is not enabled, this value specifies the time to wait without being connected to your provider before terminating the connection. To ensure that the link is always active, enter a *0* in this field. You can also enter any positive integer value in this field.

Authentication: Set the required authentication protocol. (Auto/ CHAP/ PAP)

MTU: Maximum transmit unit the DSL connection can transmit. It is a negotiated value that packets of no more than *n* bytes can be sent to the service provider. The PPPoE interface default MTU is *1492 (max)* and PPPoA default MTU is *1500 (max)*. The minimum MTU value is *64*.

On Demand: Enables On Demand mode. The connection disconnects if no activity is detected after the specified idle timeout value. When checked, this field enables the following fields:

- Idle Timeout
- Host Trigger
- Valid Rx

Default Gateway: If checked, this WAN connection acts as the default gateway to the Internet.

Enforce MTU: This feature is enabled by default. It forces all TCP traffic to conform with PPP MTU by changing TCP maximum segment size to PPP MTU. If it is disabled, you may have issues accessing some Internet sites.

Debug: Enables PPPoE connection debugging facilities. This option is used by ISP technical support and ODM/OEM testers to simulate packets going through the network from the WAN side.

PPP Unnumbered: PPP Unnumbered is a special feature. It enables the ISP to designate a block of public IP addresses to the customer where it is statically assigned on the LAN side. PPP Unnumbered is, in essence, like a bridged connection.

LAN: The LAN field is associated with the PPP Unnumbered field and is enabled when the PPP Unnumbered field is checked. You can specify the LAN group the packets need to go to when the PPP Unnumbered feature is activated.

PVC: Permanent virtual circuit. This is a fixed virtual circuit between two users. It is the public data network equivalent of a leased line. No call setup or clearing procedures are needed.

VPI: If instructed to change this, type in the VPI value for the initial connection (using PVC 0). Default = **0**.

VCI: If instructed to change this, type in the VCI value for the initial connection (using PVC 0). Default = **0**.

QoS: Quality of Service type. Select CBR (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select UBR (Unspecified Bit Rate) for applications that are non-time sensitive, such as e-mail. Select VBR (Variable Bit Rate) for burst traffic and bandwidth sharing with other applications.

PCR: Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells.

SCR: The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted.

MBS: Maximum burst size, a traffic parameter that specifies the maximum number of cells that can be transmitted at the Peak Cell Rate.

CDVT: Cell delay variation tolerance, the maximum amount of cell delay variation that can be accommodated. Cell delay variation measures the random inter-arrival times of cells within an ATM connection due to cell transfer delay caused by buffering, multiplexing, and so on.

Auto PVC: Auto-Sensing permanent virtual circuit. The overall operation of the auto-sensing PVC feature relies on end-to-end OAM pings to defined PVCs. There are two groups of PVCs: customer default PVCs which are defined by the OEM/ISP and the backup PVCs. The customer default must have 0/35 as the first default PVC. The backup list of PVCs must be of the following VPI/VCI: *0/35*, *8/35*, *0/43*, *0/51*, *0/59*, *8/43*, *8/51*, and *8/59*. The list of PVCs are defined in XML

and is configurable. The Auto-Sensing PVC feature itself is also configurable in that the auto-search mechanism can be disabled.

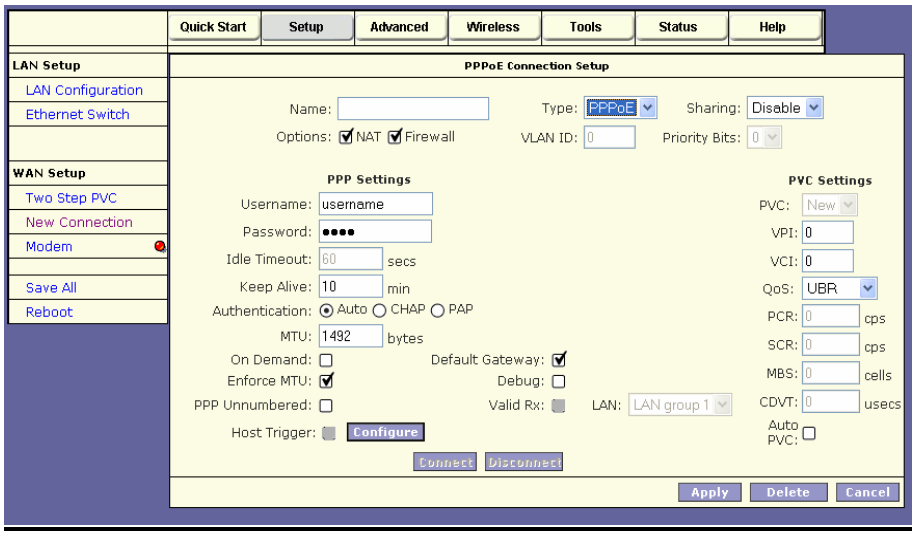
Upon DSL synchronization, end-to-end OAM pings will be conducted for every defined PVCs. The result of the pings will be recorded in an array for later use to determine the usability of the particular PVC for connectivity. This list helps the PVC manage the available PVC for use, and needs to be synchronized with connections made without Auto-Sensing PVC. Update to this list is performed for any change in DSL synchronization.

During connection establishment, the PVC module will first search through the list of defined default PVCs. If a PVC is found from the default list that is ping-able and not in use, the PVC module will update for that particular PVC as *in-use* from the list and continues processing. If a PVC is not found in the default, the backup PVC list is used. If no PVC is found again, the module will let the end-user know that no available VCC was found.

With the connection established, the PVC is stored in flash as the connection default PVC. Therefore upon reboot, this PVC is automatically chosen as the PVC for that connection. This saved PVC in environment space of flash overrides the PVC connection saved in XML configuration space of flash for that connection. During the connection establishment processing, the saved PVC will be checked to see whether a connection can be made with the PVC. If the PVC is OAM ping-able, the connection process continues. If the PVC is not OAM ping-able, the search for an available PVC starts. The process of PVC selection is the same as described above.

The list of default PVCs and backup PVCs need to be global for the management of all connections, non *Auto-Sensing PVC* connection, as well as, *Auto-Sensing PVC* connections. These lists allow the end-users to establish connectivity without keeping track of the PVC used.

PPPoE Settings

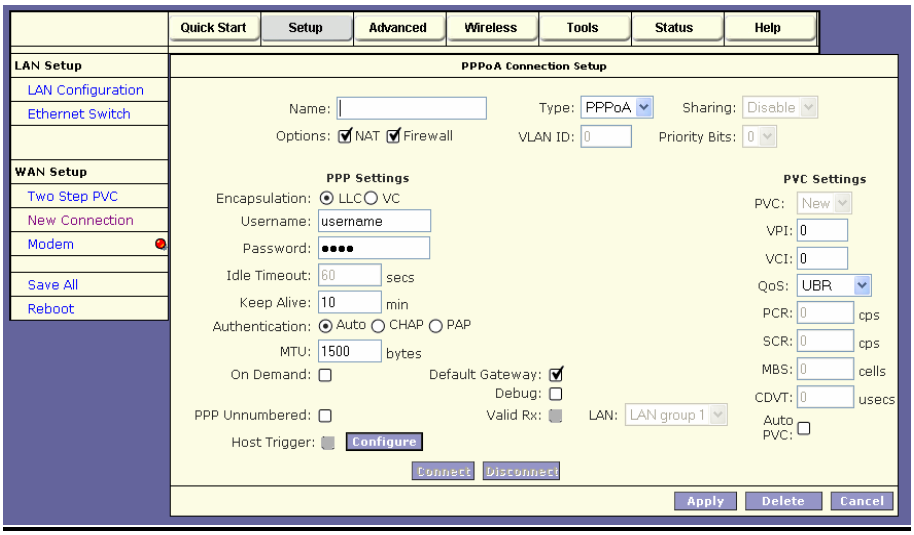


1. At the **Setup** main page, click **New Connection**.
2. At the **Type** field select **PPPoE**.
3. In the **Name** field, enter a unique name for the PPPoE connection. The name must not have spaces and cannot begin with numbers.
4. The **Network Address Translation** (NAT) and the **Firewall** options are enabled by default. Leave these in the default mode.
   Note—NAT enables the IP address on the LAN side to be translated to IP address on the WAN side. If NAT is disabled, you cannot access the Internet.
5. If you want to enable VLAN, use the reference to configure the following fields:
   • **Sharing**: Select VLAN to enable the **VLAN ID** and **Priority Bits** fields.
   • **VLAN ID**: Enter the VLAN ID.
   • **Priority Bits**: Select the priority bits of the VLAN.
6. In the **PPP Settings** section, enter values from DSL service provider or your ISP.
7. In the **PVC Settings** section, enter values for the **VPI** and **VCI**.
   Note—Your DSL service provider or your ISP supplies these values.
8. Select the **Quality of Service** (QoS). Leave the default value if you are unsure or if the ISP did not provide this information.
   The **PCR**, **SCR**, **MBS**, and **CDVT** fields are enabled / disabled depending on the **QoS** selection. Enter the values provided by the ISP or leave the defaults.
9. Click **Apply** to complete the connection setup.

Sharing	The following options are available: • **Disable**: Disables connection sharing. • **Enable**: Enables connection sharing. • **VLAN**: The **VLAN ID** and **Priority Bits** fields are activated when VLAN is selected, which enable you to create VLAN.
VLAN ID	VLAN Identification. Multiple connections over the same PVC are Supported, which requires the WAN network to have VLAN support and for

	the DSLAMS and Routers on the ISP to handle VLAN Tags. Extended support is also available, which allows multiple connections to be placed over the single PVC without VLAN support (VLAN Tag of *0* is this special case). In this mode of operation, a received packet is flooded on all the connections that reside over it.
Priority Bits	Priority is given to a VLAN connection from *0-7*. All packets sent over the VLAN connection have the Priority bits set to the configured value.

PPPoA Settings

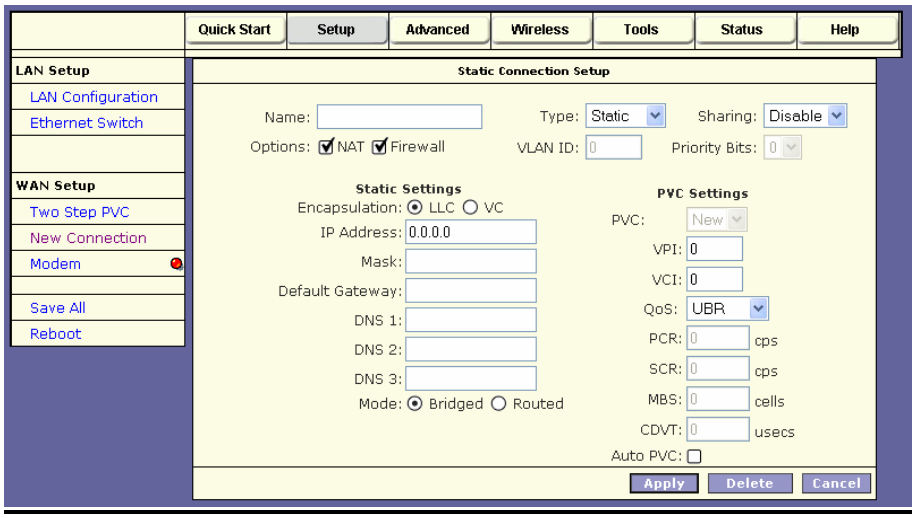


1. At the **Setup** main page, click **New Connection**.
2. At the **Type** field select **PPPoA**.
3. Enter a unique name for the PPPoA connection in the **Name** field. The name must not have spaces and cannot begin with numbers.
4. The **Network Address Translation** (NAT) and the **Firewall** options are enabled by default. Leave these in the default mode.
5. If you want to enable VLAN, use the reference to configure the following fields:
   - **Sharing**: Select VLAN to enable the **VLAN ID** and **Priority Bits** fields.
   - **VLAN ID**: Enter the VLAN ID.
   - **Priority Bits**: Select the priority bits of the VLAN.
6. In the **PPP Settings** section, select the encapsulation type (LLC or VC).
   Note— If you are not sure, just use the default mode.
7. In the **PVC Settings** section, enter values for the **VPI** and **VCI**.
   Note—Your DSL service provider or your ISP supplies these values.
8. Select the **Quality of Service** (QoS). Leave the default value if you are unsure or if the ISP did not provide this information.
   The **PCR**, **SCR**, **MBS**, and **CDVT** fields are enabled / disabled depending on the **QoS** selection. Enter the values provided by the ISP or leave the defaults.
9. Click **Apply** to complete the connection setup.

Sharing	The following options are available: • **Disable**: Disables connection sharing. • **Enable**: Enables connection sharing. • **VLAN**: The **VLAN ID** and **Priority Bits** fields are activated when VLAN is selected, which enable you to create VLAN.
VLAN ID	VLAN Identification. Multiple connections over the same PVC are Supported, which requires the WAN network to have VLAN support and for the DSLAMS and Routers on the ISP to handle VLAN Tags. Extended

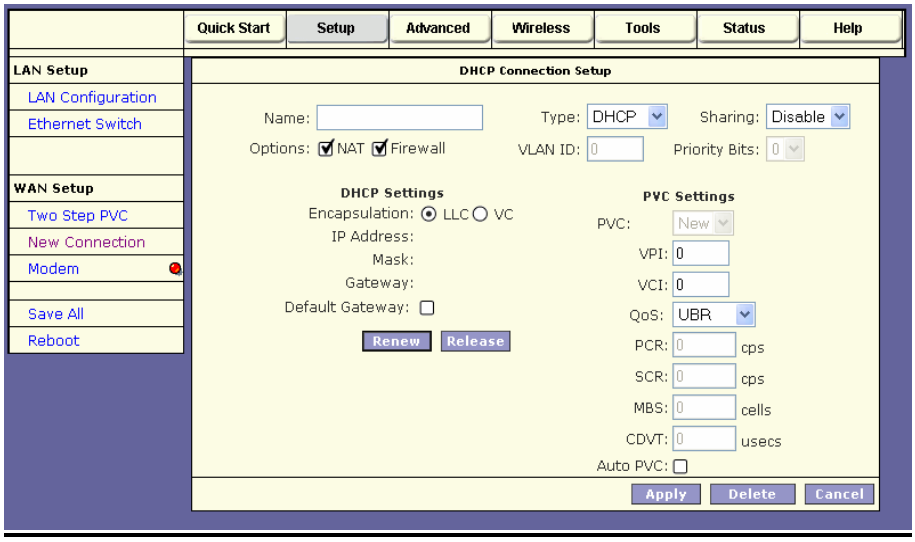
	support is also available, which allows multiple connections to be placed over the single PVC without VLAN support (VLAN Tag of *0* is this special case). In this mode of operation, a received packet is flooded on all the connections that reside over it.
Priority Bits	Priority is given to a VLAN connection from *0-7*. All packets sent over the VLAN connection have the Priority bits set to the configured value.

Static Settings



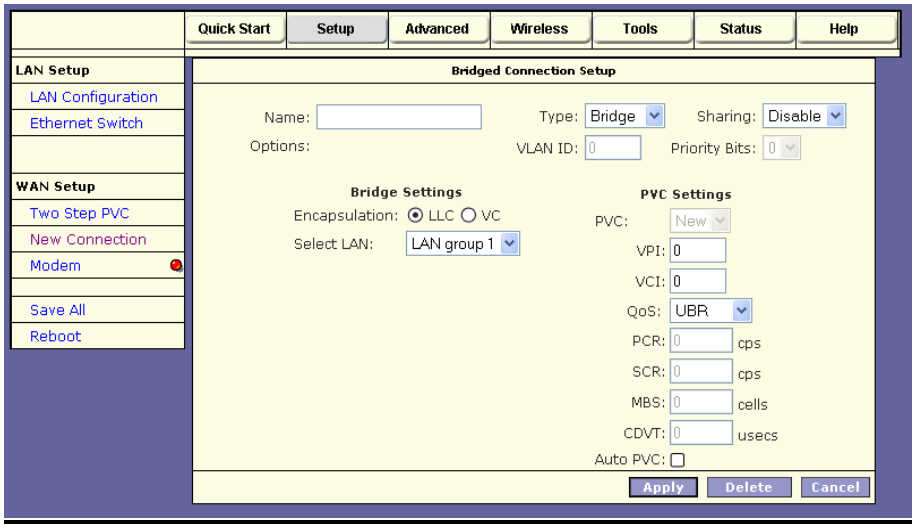
1. At the **Setup** main page, click **New Connection**.
2. At the **Type** field select **Static**.
3. In the **Name** field, enter a unique name for the Static connection.
   The name must not have spaces and cannot begin with numbers.
4. The **Network Address Translation** (NAT) and the **Firewall** options are enabled by default. Leave these in the default mode.
5. In the **Static Settings** section, select the **Encapsulation Type** (LLC or VC).
   Note— If you are not sure, just use the default mode.
6. Based upon the information your DSL/ISP provided, enter your assigned **IP Address**, **Subnet Mask**, **Default Gateway** (if provided), and **Domain Name Services** (DNS) values (if provided).
7. For the static configuration, you can also select a **Bridged** connection or a **Routed** connection.
8. In the **PVC Settings** section, enter values for the **VPI** and **VCI**.
   Note—Your DSL service provider or your ISP supplies these values.
9. Select the **Quality of Service** (QoS). Leave the default value if you are unsure or if the ISP did not provide this information.
   The PCR, **SCR**, **MBS**, and **CDVT** fields are enabled / disabled depending on the **QoS** selection. Enter the values provided by the ISP or leave the defaults.
10. Click **Apply** to complete the connection setup.

DHCP Settings



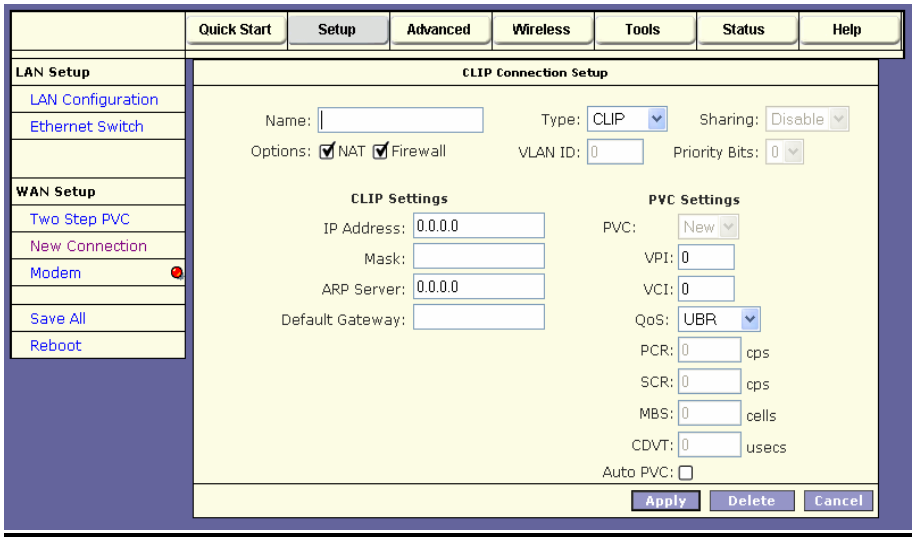
1. At the **Setup** main page, click **New Connection**.
2. At the **Type** field select **DHCP**.
3. Enter a unique name for the DHCP connection in the **Name** field.
   The name must not have spaces and cannot begin with numbers.
4. The **Network Address Translation** (NAT) and the **Firewall** options are enabled by default. Leave these in the default mode.
5. If your DSL line is connected and your DSL/IPS provider is supporting DHCP, you can click **Renew** and the gateway retrieves an IP Address, Subnet Mask, and Gateway Address. At any time, you can release the DHCP address by clicking **Release**, and renew the DHCP address by clicking **Renew**.
6. Under **PVC Settings**, enter values for the **VPI** and **VCI**.
   Note—Your DSL service provider or your ISP supplies these values.
7. Select the **Quality of Service** (QoS). Leave the default value if you are unsure or if the ISP did not provide this information.
   The **PCR**, **SCR**, **MBS**, and **CDVT** fields are enabled / disabled depending on the **QoS** selection. Enter the values provided by the ISP or leave the defaults.
8. Click **Apply** to complete the connection setup.

Bridge Settings



1. At the **Setup** main page, click **New Connection**.
2. At the **Type** field select **Bridge**.
3. Enter a unique name for the Bridged connection in the **Name** field. The name must not have spaces and cannot begin with numbers.
4. In the **Bridge Settings** section, select the **Encapsulation Type** (LLC or VC).
   Note— If you are not sure, just use the default mode.
5. In the **PVC Settings** section, enter values for the **VPI** and **VCI**.
   Note—Your DSL service provider or your ISP supplies these values.
6. Select the **Quality of Service** (QoS). Leave the default value if you are unsure or if the ISP did not provide this information.
   The **PCR**, **SCR**, **MBS**, and **CDVT** fields are enabled / disabled depending on the **QoS** selection. Enter the values provided by the ISP or leave the defaults.
7. Click **Apply** to complete the connection setup.

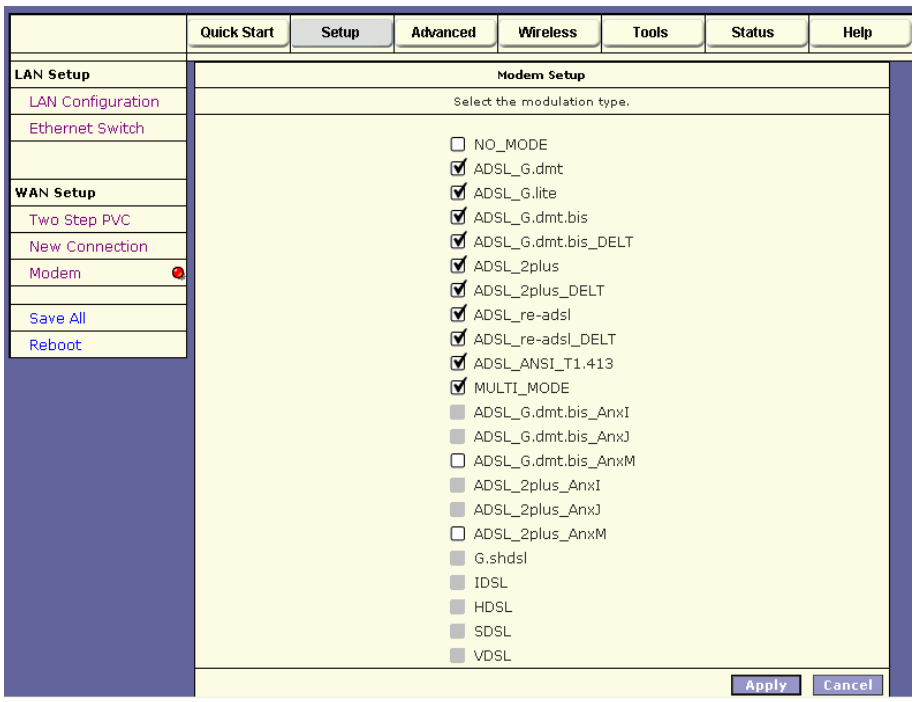
CLIP Settings



1. At the **Setup** main page, click **New Connection**.
2. At the **Type** field select **CLIP**.
3. Enter a unique name for the static connection in the **Name** field. The name must not have spaces and cannot begin with numbers.
4. The **Network Address Translation** (NAT) and the **Firewall** options are enabled by default. Leave these in the default mode.
5. Based upon the information your DSL/ISP provided, enter your assigned **IP Address**, **Mask**, **ARP Server**, and **Default Gateway**.
6. In the **PVC Settings** section, enter values for the **VPI** and **VCI**.
   Note—Your DSL service provider or your ISP supplies these values.
7. Select the **Quality of Service** (QoS); leave the default value if you are unsure or if the ISP did not provide this information.
   The **PCR**, **SCR**, **MBS**, and **CDVT** fields are enabled / disabled depending on the **QoS** selection. Enter the values provided by the ISP or leave the defaults.
8. Click **Apply** to complete the connection setup.

Modem

This page allows you Select ADSL Transmission Type.



MULTI_MODE: Support Multi-Mode standard (ANSI T1.413 Issue 2; G.dmt(G.992.1); G.lite(G.992.2)).

ADSL_ANSI_T1.413: Full-Rate (ANSI T1.413 Issue 2) with line rate support of up to 8 Mbps downstream and 832 Kbps upstream.

ADSL_G.dmt: Full-Rate (G.dmt, G992.1) with line rate support of up to 8 Mbps downstream and 832 Kbps upstream.

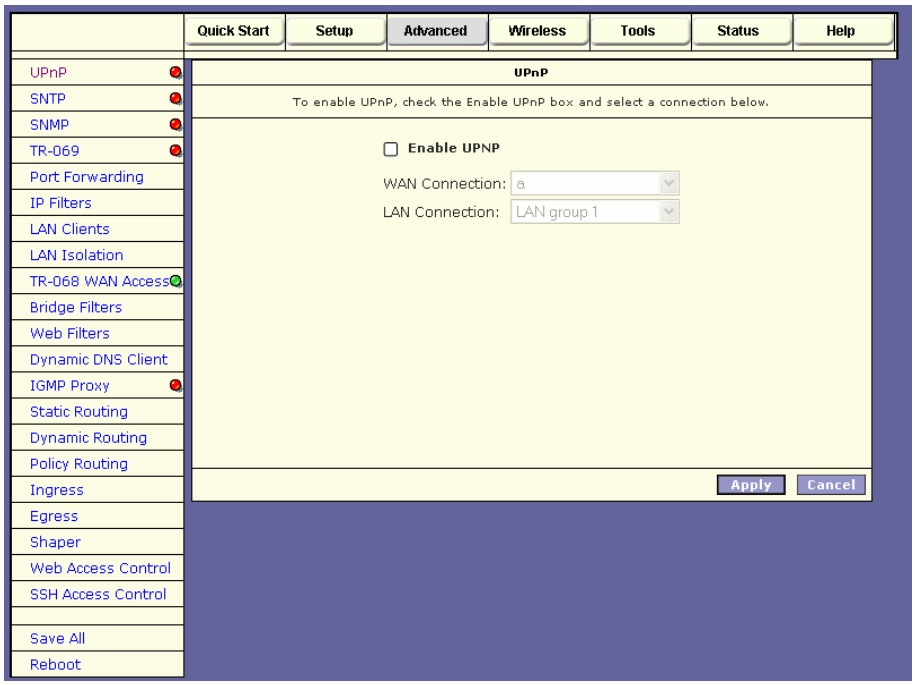
ADSL_G.lite: G.lite (G.992.2) with line rate support of up to 1.5 Mbps downstream and 512 Kbps upstream.

Click ***Apply*** to complete the setup. Click ***Save All*** to save the changes.

ADVANCED

UPnP

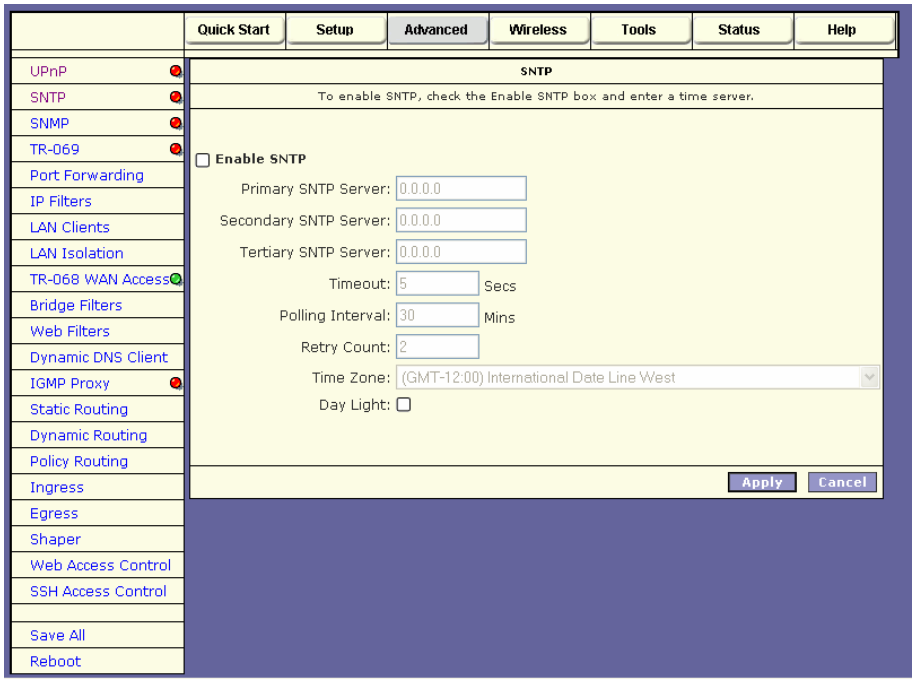
Universal plug and play (UPnP), NAT, and firewall traversal allow traffic to pass through the RG for applications using the UPnP protocol. This feature requires one active WAN connection. In addition, the PC should support this feature. In the presence of multiple WAN connections, select a connection on which the incoming traffic is present, for example, the default WAN connection.



1. Check **Enable UPnP**.
   This enables the WAN Connection and LAN Connection fields.
2. Select the **WAN Connection** and **LAN Connection** that will use UPnP from the drop-down lists.
3. Click **Apply** to temporarily activate the settings.
   Note— The changes take effect when you click **Apply**; however, if the RG configuration is not saved, these changes will be lost upon RG reboot.
4. To make the change permanent, click **Tools** (at the top of the page) and select **System Commands**.
5. On the **System Commands** page, click **Save All**.

SNTP

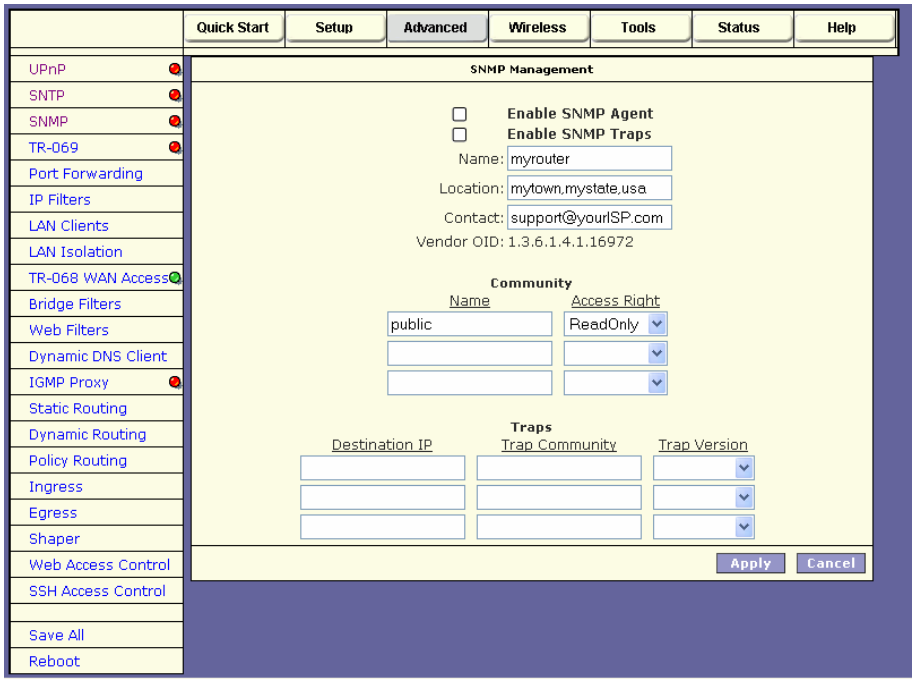
The Router keeps time by connecting to a Simple Network Time Protocol (SNTP) server. This allows the Router to synchronize the system clock to the global Internet. The synchronized clock in the Router is used to record the security log and control client filtering.



Primary SNTP Server: Enter the SNTP Server address. Default is 0.0.0.0.
Secondary SNTP Server: Enter the SNTP Server address. Default is 0.0.0.0.
Tertiary SNTP Server: Enter the SNTP Server address. Default is 0.0.0.0.
Timeout: Timeout (secs) for response to SNTP request.
Polling Interval: Time interval (min) between two successful SNTP requests.
Retry Count: Max. no of failed sntp requests to a server.
Time Zone: Time zone of the location.
Day Light: Daylight savings feature enabled (1) or disabled (0). Default disabled.
Click ***Apply*** to complete the setup. Click ***Save All*** to save the changes.

SNMP

The Simple Network Management Protocol (SNMP) let a network administrator monitor on a network by retrieving settings on remote network devices. Network administrator typically runs an SNMP management station program such as MIB browser on a local host to obtain information from an SNMP agent such as the router you use now.



Name: Enter information about the system name in the system contact field.

Location: Enter information about the system contact person in the system contact field.

Contact: Enter information about the system contact person in the system contact field.

Vendor OID: The enterprise OID to which the system belongs to.

Click ***Apply*** to complete the setup. Click ***Save All*** to save the changes.

TR-069

TR-069 is CPE Management Protocol from WAN side, intended for communication between a CPE and Auto-Configuration Server (ACS). The CPE WAN Management Protocol defines a mechanism that encompasses secure auto-configuration of a CPE, and also incorporates other CPE management functions into a common framework.

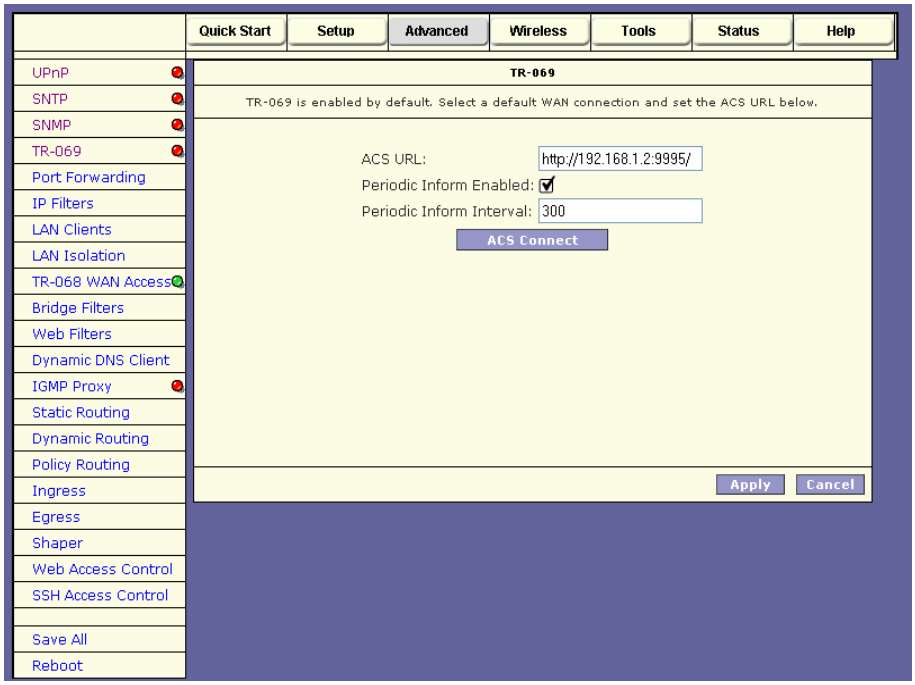
The CPE WAN Management Protocol is intended to support a variety of functionalities to manage a collection of CPE, including the following primary capabilities:

•Auto-configuration and dynamic service provisioning

•Software/firmware image management

•Status and performance monitoring

•Diagnostic



ACS URL: URL of the auto configuration server (ACS) provided by the ISP.

Periodic Inform Enabled: Enable/disables the RG to connect to the ACS periodically. If you enable this feature, you should enter a value in the Periodic Inform Interval field.

Periodic Inform Interval: This field is enabled only when the Periodic Inform Enabled field is checked. It defines the amount of time (in seconds) between a successful connection with an ACS server and a new attempt to connect to an ACS server. A recommended value is 86400 seconds (1 day).

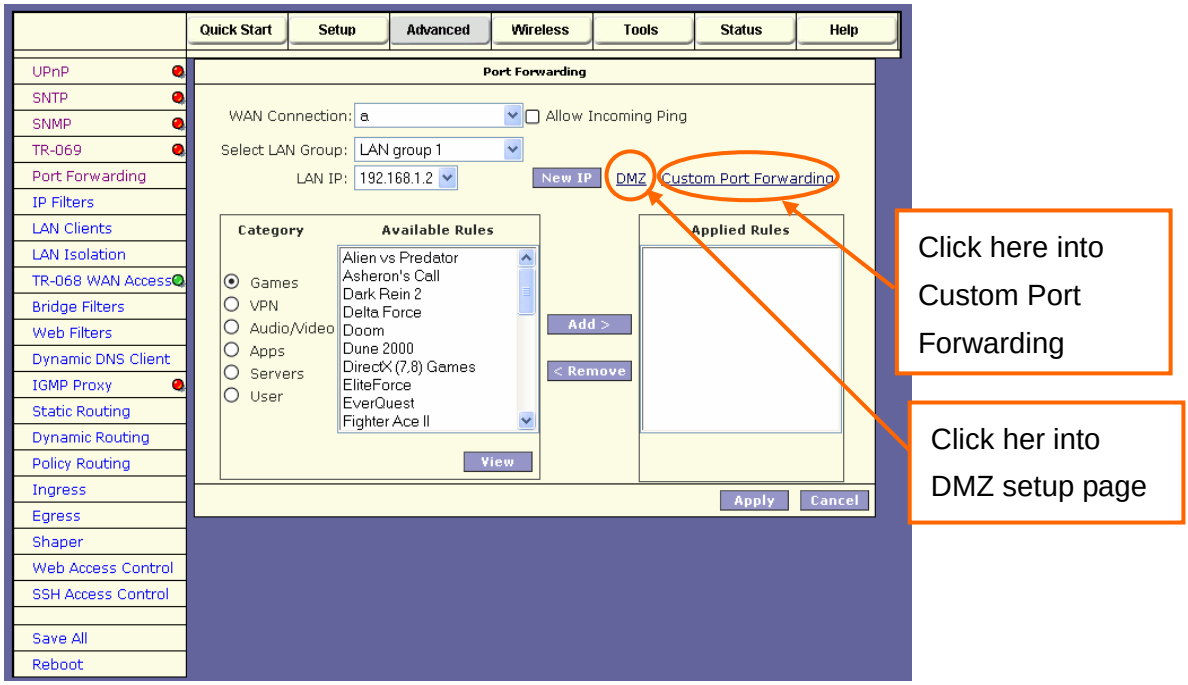
ACS Connect: By clicking the ACS Connect button, you manually connect the RG to the ACS.

Click ***Apply*** to complete the setup. Click ***Save All*** to save the changes.

Port Forwarding

The port forwarding feature allows you to direct incoming traffic to specific LAN hosts based on a protocol port number and protocol. Using the **Port Forwarding** page, you can provide local services (for example, web hosting) for people on the Internet or play Internet games. Port forwarding is configurable per LAN group.

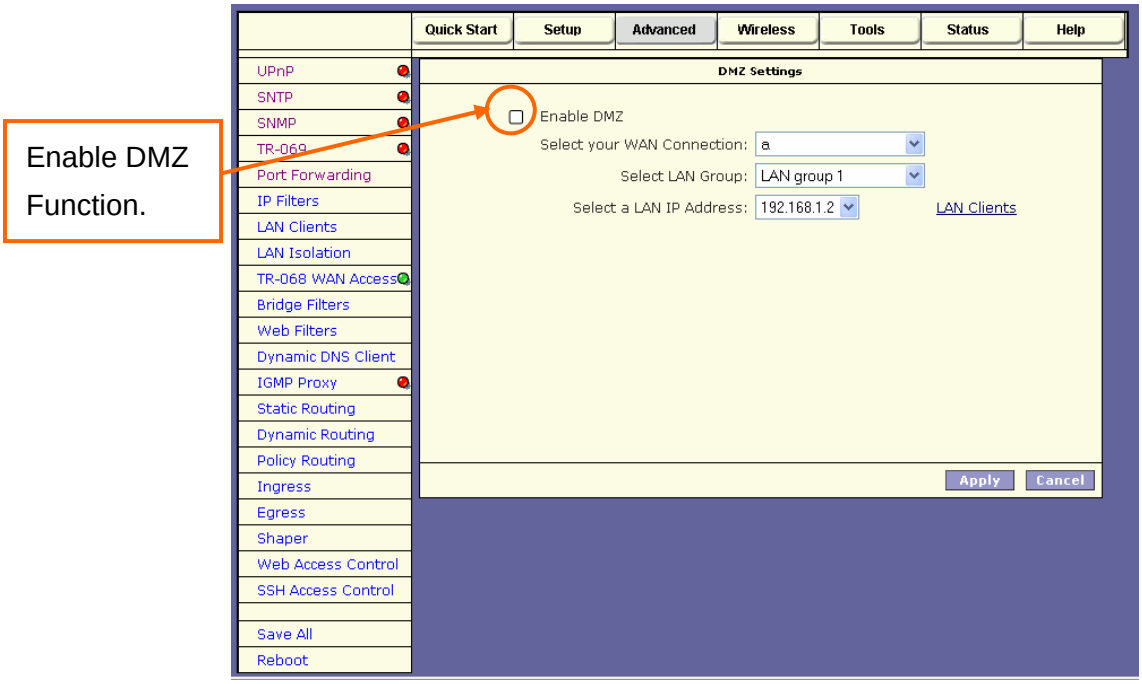
A database of predefined port forwarding rules allows you to apply one or more rules to one or more members of a defined LAN group. You can view the rules associated with a predefined category and add the available rules for a given category. You can also create, edit, or delete your own port forwarding rules.



WAN Connection: Select the WAN connection to which port forwarding is applied.
Select LAN Group: Select the LAN Group to which port forwarding is applied.
LAN IP: Select the IP address to host the service.
Allow Incoming Ping: Enabling incoming ping (ICMP) requests on the **Port Forwarding** page allows the RG to respond to a ping from the Internet.
DMZ: Demilitarized zone.
Custom Port Forwarding: This link takes you to the **Custom Port Forwarding** page.
Category: Custom and user-defined categories.
Available Rules: Predefined and user-defined IP filtering rules for each category.
Applied Rules: Lists the IP filtering rules you elect to apply for each given category.
Click ***Apply*** to complete the setup. Click ***Save All*** to save the changes.

DMZ

This DMZ Settings page allows you Enable or Disable this function. This function is disabled by default. By enabling DMZ, you add an extra layer of security protection for hosts behind the firewall.



Enable DMZ: Enables/disables the Demilitarized Zone feature. This field is unchecked (disabled) by default.

Select your WAN Connection: Select the WAN connection on which the DMZ feature is applied.

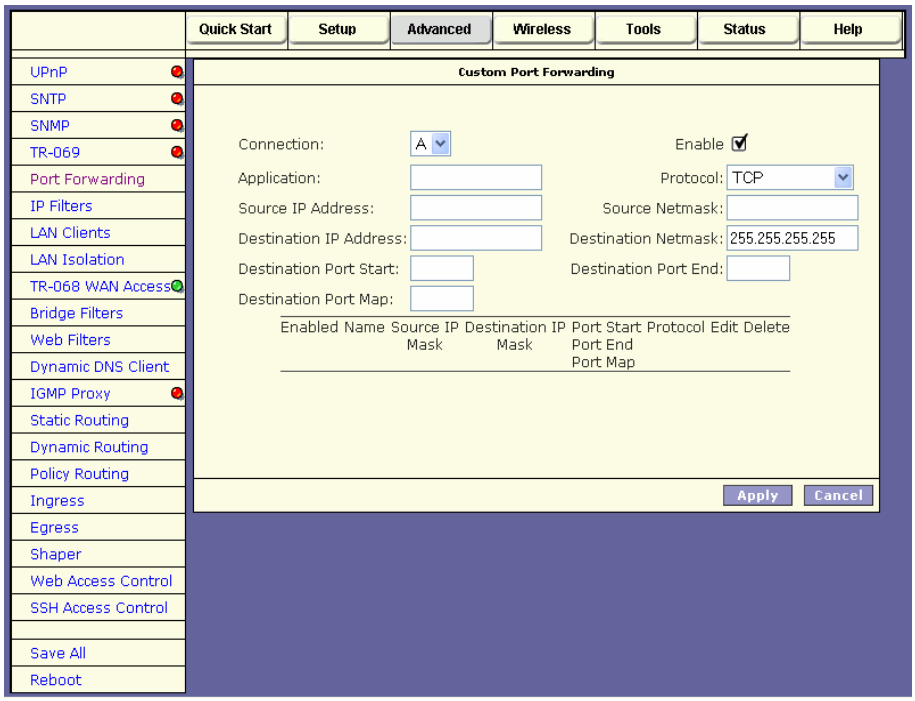
Select LAN Group: Select the LAN Group on which the DMZ feature is applied.

Select a LAN IP Address: Select the LAN IP address you are going to use as the DMZ host. This host is exposed to the Internet. Be aware that this feature may expose your local network to security risks.

Click ***Apply*** to complete the setup. Click ***Save All*** to save the changes.

Custom Port Forwarding

The Custom Port Forwarding page allows you to create up to 15 custom port forwarding entries to support specific services or applications, such as concurrent NAT/NAPT operation.



Connection: Select the WAN connection on which the Custom Port Forwarding rule is to be applied.

Enable: The Enable button is checked by default, meaning this rule is automatically applied when you click the Apply button.

Application: Name of the application for which your ports will be opened.

Protocol: There are three options available: *TCP*, *UDP*, and *TCP and UDP*.

Source IP Address: You can define the source IP address from which the incoming traffic is allowed. Enter *0.0.0.0* for all.

Source Netmask: Netmask of the source IP address. Enter *255.255.255.255* for all.

Destination IP Address: The LAN-side destination IP address for incoming traffic.

Destination Netmask: The LAN-side destination netmask for incoming traffic. The default value of this field is *255.255.255.255*.

Destination Port Start: The starting port number that is made open for this application.

Destination Port End: The ending port number that is made open for this application.

Destination Port Map: Destination port mapped on the LAN (destination) side to which packets are forwarded. There are two types of port mapping:

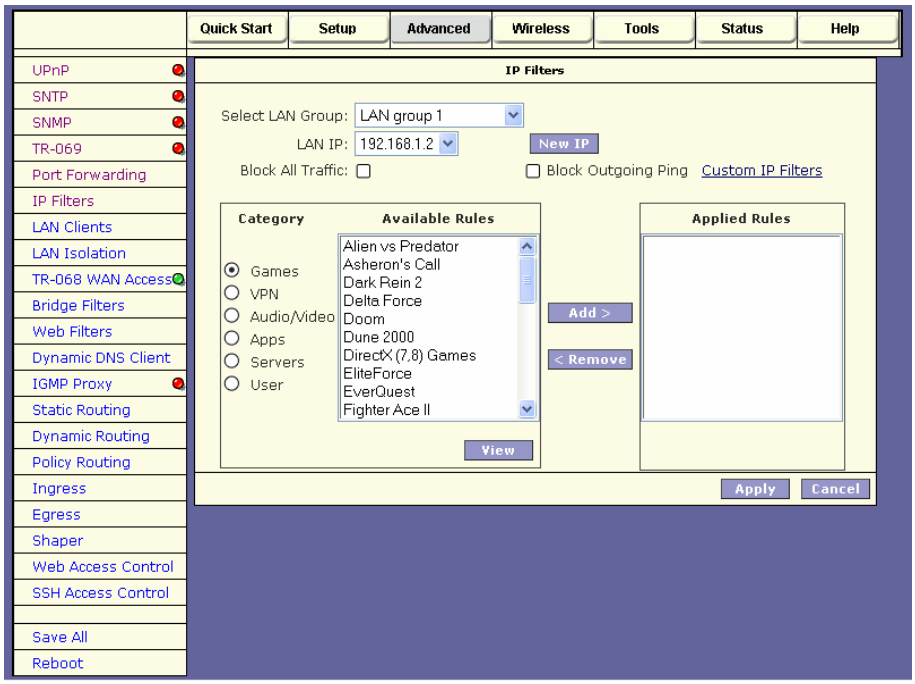
- One-to-one (one port mapped to one)
- Multiple-to-one (multiple ports mapped to one port)

Click Apply to complete the setup. Click Save All to save the changes.

IP Filter

The IP filtering feature allows you to block specific applications/services based on the IP address of a LAN device. You can use the **IP Filters** page to block specific traffic (for example, block web access) or any traffic from a host on your local network.

A database of predefined IP filters allows you to apply one or more filtering rules to one or more members of a defined LAN group. You can view the rules associated with a predefined filter and add the available rules for a given category. You can also create, edit, or delete your own IP filter rules.



Select LAN Group: Select the LAN group to which the IP filters feature will be applied.

LAN IP: Select the IP address in the given LAN group to which the IP Filters feature will be applied.

Block All Traffic: When checked, complete network access is blocked for the specific IP address.

Block Outgoing Ping: Blocking outgoing ping (ICMP) generated from a particular LAN IP can be used if your host has a virus that attempts a Ping-of-Death Denial of Service attack.

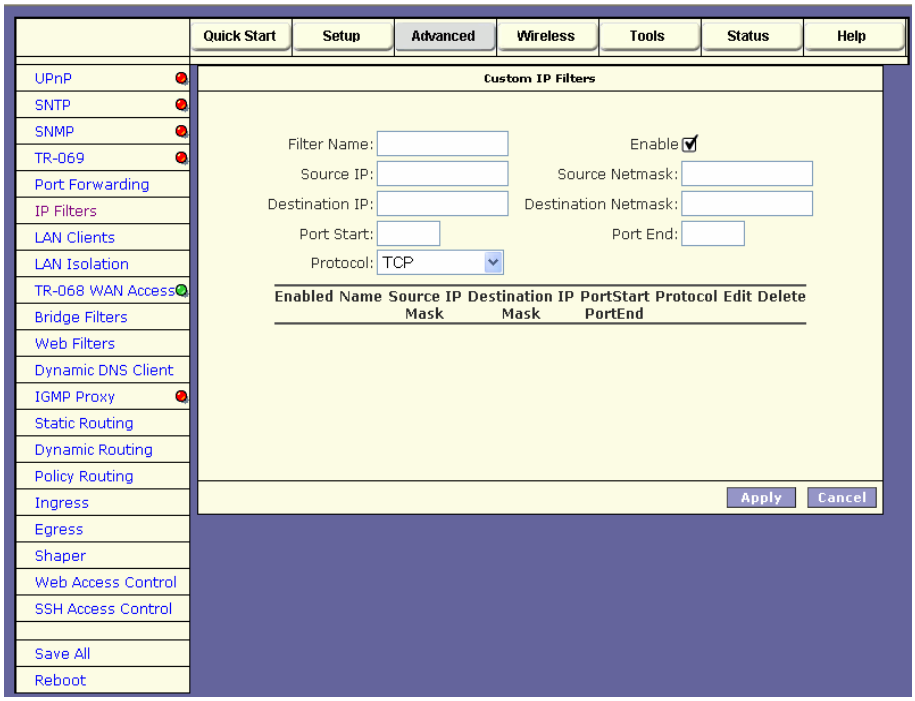
Click Apply to complete the setup. Click Save All to save the changes.

Custom IP Filters

The Custom IP Filters page allows you to define up to 20 custom IP filtering entries to block specific services or applications based on:

- Source/destination IP address and netmask
- TCP port (ranges supported)
- Protocol

• TCP
• UDP
• TCP and UDP
• ICMP
• Any



Filter Name: Name of the IP filter rule you are creating.

Enable: The Enable button is checked by default, meaning this rule is automatically applied when you click Apply.

Source IP: The LAN-side source IP address assigned to outgoing traffic on which filtering is applied.

Source Netmask: Netmask of the source IP on your LAN side.

Destination IP: You can define the destination IP address to which your source IP will be banned access. Enter *0.0.0.0* for all.

Destination Netmask: Netmask of the destination IP. Enter *255.255.255.255* for all.

Port Stat: The starting port number that will be blocked for this application.

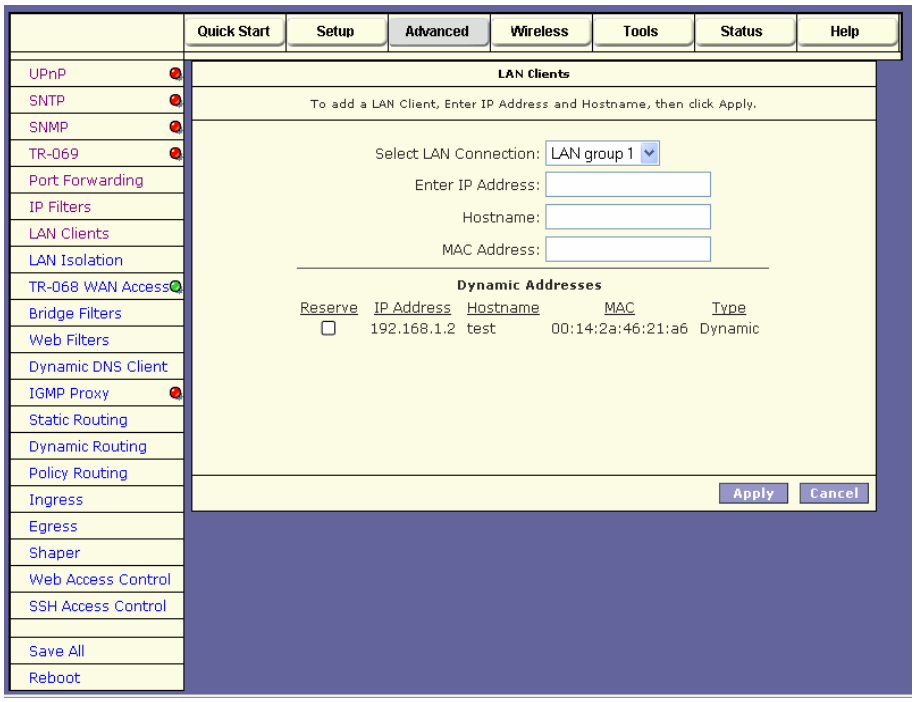
Port End: The ending port number that will be blocked for this application.

Protocol: There are five options available: *TCP*, *UDP*, *TCP and UDP*, *ICMP*, and *Any*.

Click ***Apply*** to complete the setup. Click ***Save All*** to save the changes.

LAN Clients

The LAN clients feature allows you to see all the hosts on the LAN segment. Each host is qualified to be either dynamic (host obtained a lease from this RG) or static (host has a manually-configured IP address).



Select LAN Connection: Select the LAN connection to which the client is to be added.

Enter IP Address: Assign the dynamic IP address to the host here. This is a mandatory field.

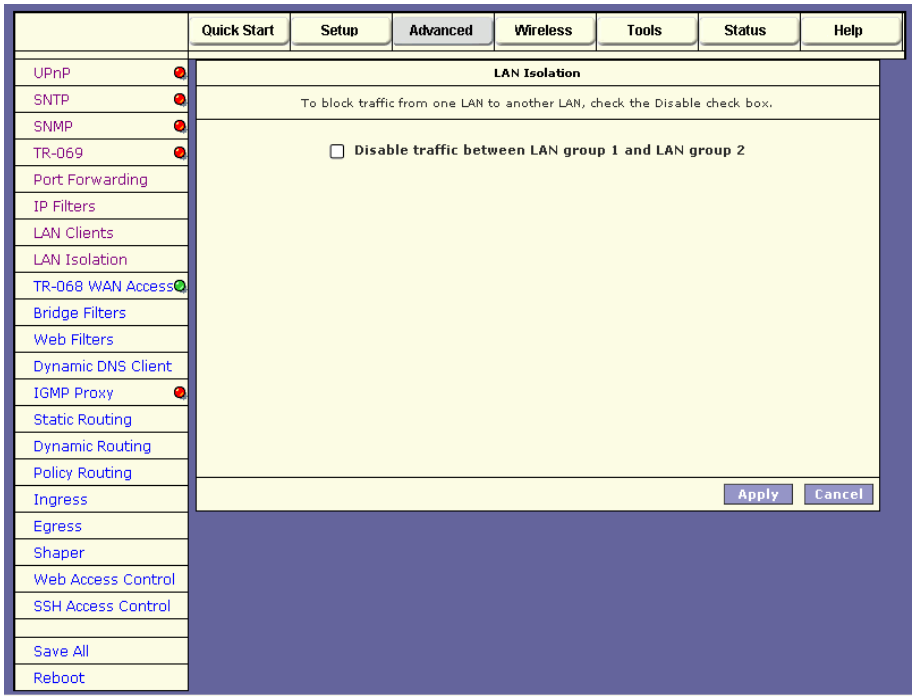
Hostname: Hostname of the client. This is an optional field.

MAC Address: MAC address of the host. This is an optional field.

Click ***Apply*** to complete the setup. Click ***Save All*** to save the changes.

LAN Isolation

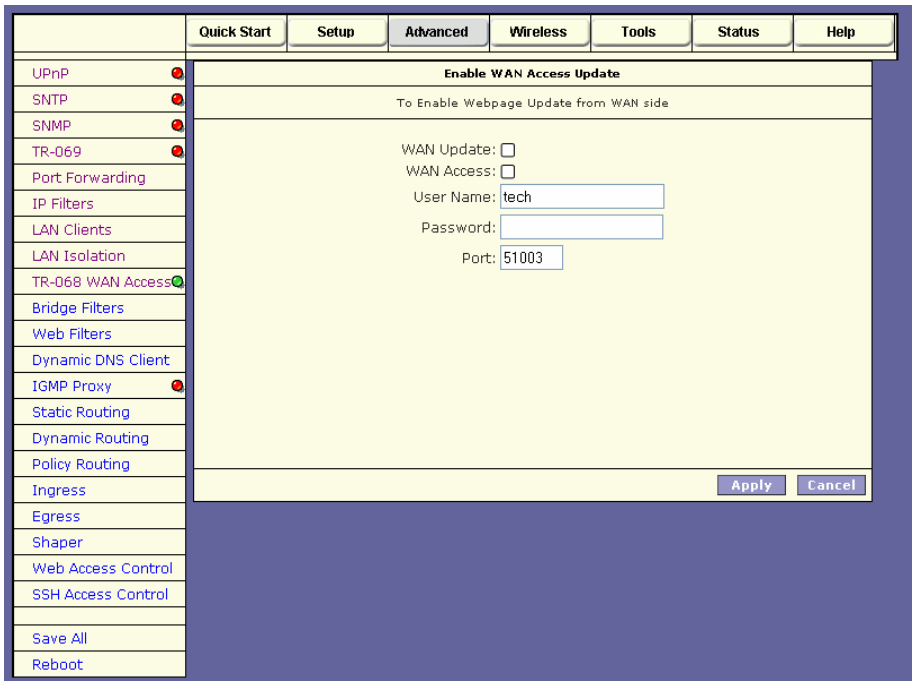
The LAN Isolation page allows you to block traffic from one LAN group to another LAN group.



Click ***Apply*** to complete the setup. Click ***Save All*** to save the changes.

TR-068 WAN Access

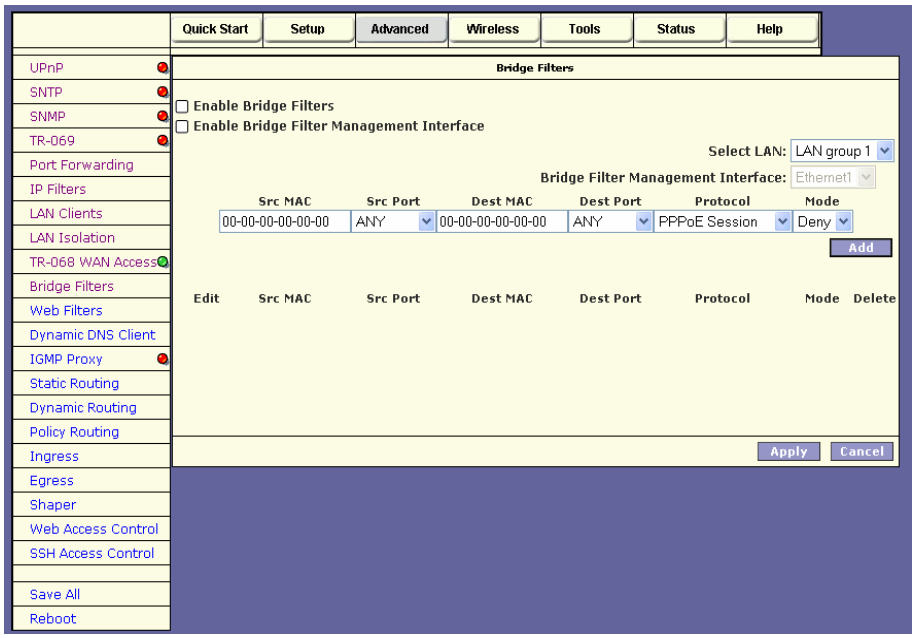
The TR-068 WAN Access page enables you to give temporary permission to someone (such as technical support staff) to be able to access your RG from the WAN side. From the moment the account is enabled, the user is expected to log in within 20 active minutes, otherwise the account expires. Once the user has logged in, if the session remains inactive for more than 20 minutes, the user will be logged out and the account expires.



WAN Update: Check this field to give the account read and writes access.
WAN Access: Check this field to give the account read-only access.
User Name: User name of the WAN access account.
Password: Password of the WAN access account.
Port: Enter the port number to be opened for the temporary WAN access.
Click ***Apply*** to complete the setup. Click ***Save All*** to save the changes.

Bridge Filters

The bridge filtering mechanism provides a way for you to define rules to allow or deny frames through the bridge based on source MAC address, destination MAC address, frame type, and physical ports. When bridge filtering is enabled, each frame is examined against every defined filter rule in sequence. When a match is found, the appropriate filtering action (allow or deny) is performed. Note that the bridge filter only examines frames from interfaces that are part of the bridge itself. Up to 20 filter rules are supported with bridge filtering.



Enable Bridge Filters: Enables/disables bridge filtering. It can be set/unset during any add, *edit*, or *delete* operation. It can also be set / unset independently by clicking **Apply**.

Enable Bridge Filter Management Interface: When checked, it enables the Bridge Filter Management Interface field. This ensures that you do not get locked out of the RG on the interface of the LAN group specified in the next two fields.

Select LAN: Select your LAN group to enable the Bridge Filter Management Interface feature.

Bridge Filter Management Interface: Select the interface of the LAN group to have the Bridge Filter Management Interface feature enabled. Depending on the LAN group that is selected, the interface selections are *Ethernet*, *USB*, and/or *WLAN*.

SRC MAC: The source MAC address. It must be in a *xx-xx-xx-xx-xx-xx* format, with *00-00-00-00-00-00* as *don't care*. Blanks can be used in the MAC address space and are also considered as *don't care*.

SRC Port: Source port. You can choose from *Any*, *Ethernet*, *USB*, *WLAN*, or *WAN Bridge Connection Port* for the particular bridge. If any of the selections are not available, please check your DSL connection.

Dest MAC: The destination MAC address.

Dest Port: Destination port. You can choose from *Any*, *Ethernet*, *USB*, and *WLAN*.

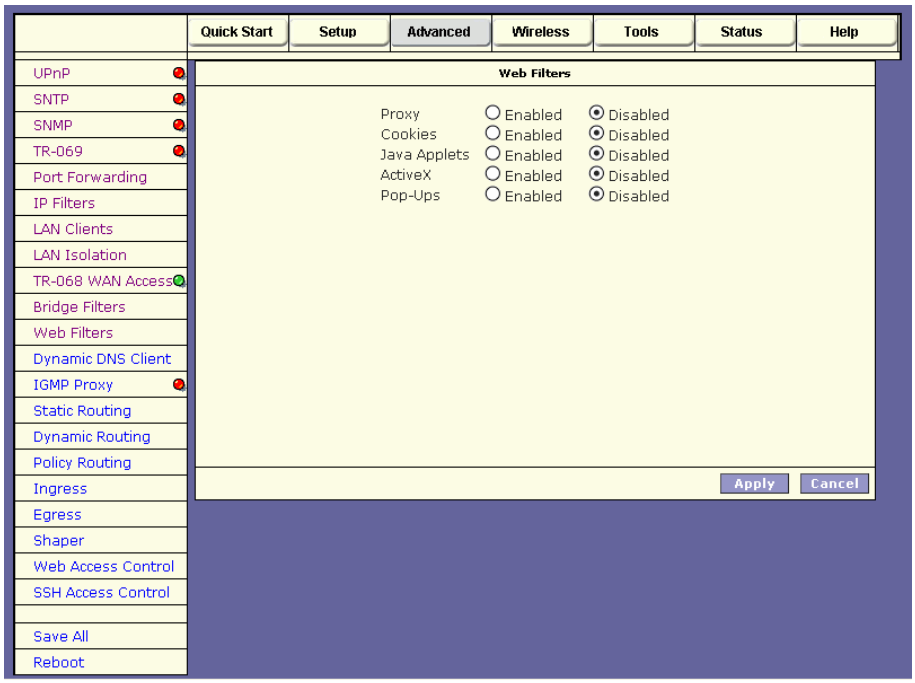
Protocol: You can choose from the following options: *PPPoE Session*, *PPPoE Discovery*, *IPX - Ethernet II*, *RARP*, *IPv6*, *IPv4*, and *Any*.

Mode: There are two filtering modes: *Deny* and *Allow*.

Click ***Apply*** to complete the setup. Click ***Save All*** to save the changes.

Web Filters

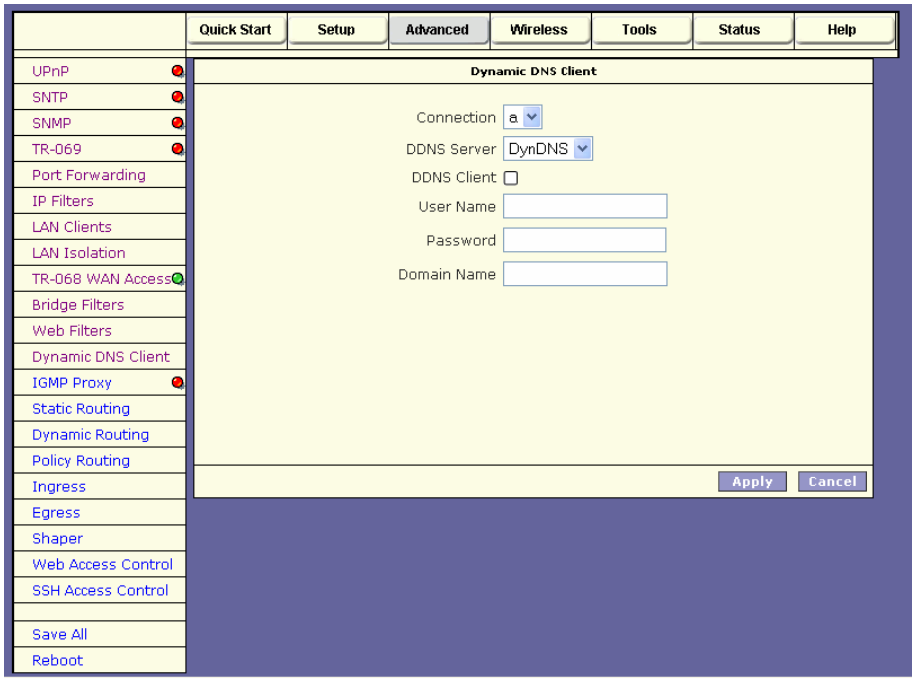
The **Web Filters** page allows you to manage the type of web content that passes through your RG.



Click ***Apply*** to complete the setup. Click ***Save All*** to save the changes.

Dynamic DNS Client

The Dynamic DNS Client page allows you to enable/disable the Dynamic DNS feature.



Connection: This field defaults to your RG's WAN connection over which your RG will be accessed.

DDNS Server: This is where you select the server from different DDNS service providers. A charge may occur depends on the service you select.

DDNS Client: Enables/disables the DDNS client feature for the WAN connection. This field is disabled by default.

User Name: User name assigned by the DDNS service provider.

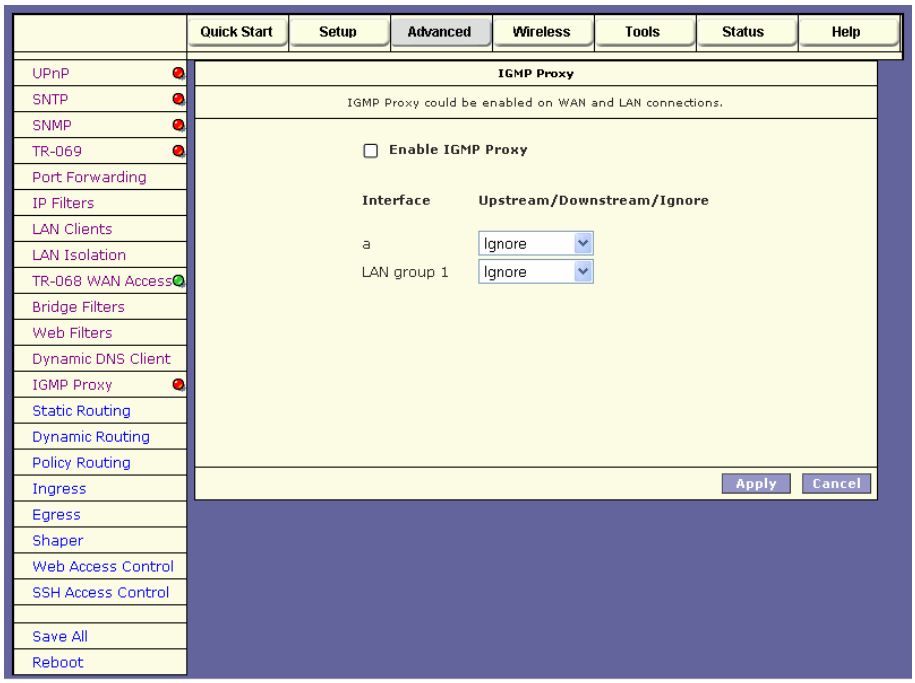
Password: Password assigned by the DDNS service provider.

Domain Name: Domain name to be registered with the DDNS server.

Click ***Apply*** to complete the setup. Click ***Save All*** to save the changes.

IGMP Proxy

The IGMP Proxy page allows you to enable multicast on available WAN and LAN connections. You can configure the WAN or LAN interface as one of the following:



Upstream: The interface that IGMP requests from hosts is sent to the multicast router.

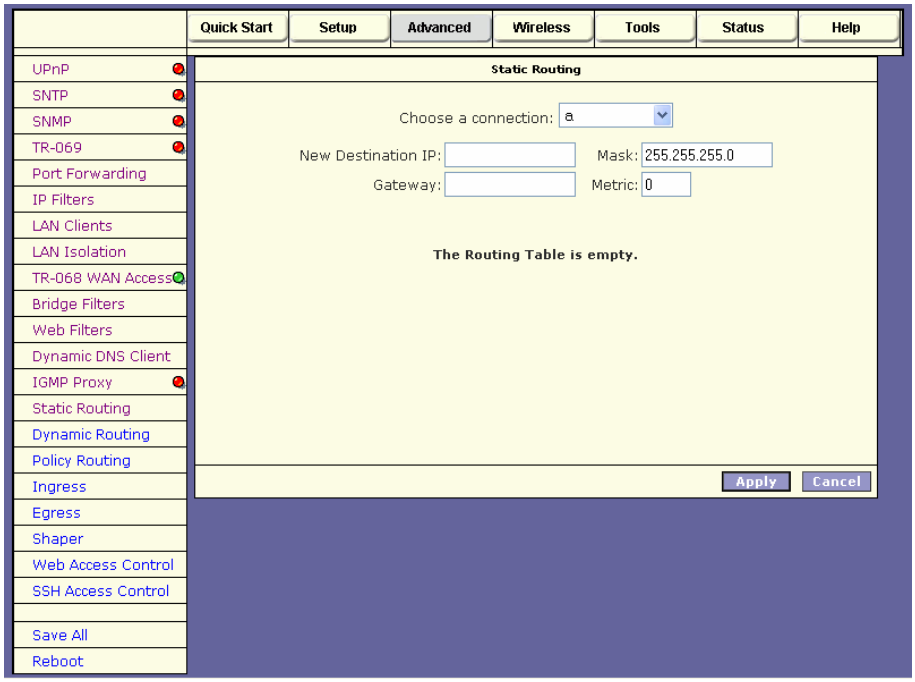
Downstream: The interface data from the multicast router are sent to hosts in the multicast group database.

Ignore: No IGMP request nor data multicast are forwarded.

Click ***Apply*** to complete the setup. Click ***Save All*** to save the changes.

Static Routing

The **Static Routing** page enables you to define routes for specific subnets on the WAN/LAN side. The RG allows you to manually program the RG's routing table. Up to 16 static routes can be added.



Choose a Connection: Select the LAN group or WAN connection to which a static routing *subnet* is to be applied.

New Destination IP: The network IP address of the subnet. (You can also enter the IP *address* of each individual station in the subnet).

Mask: The network mask of the destination subnet.

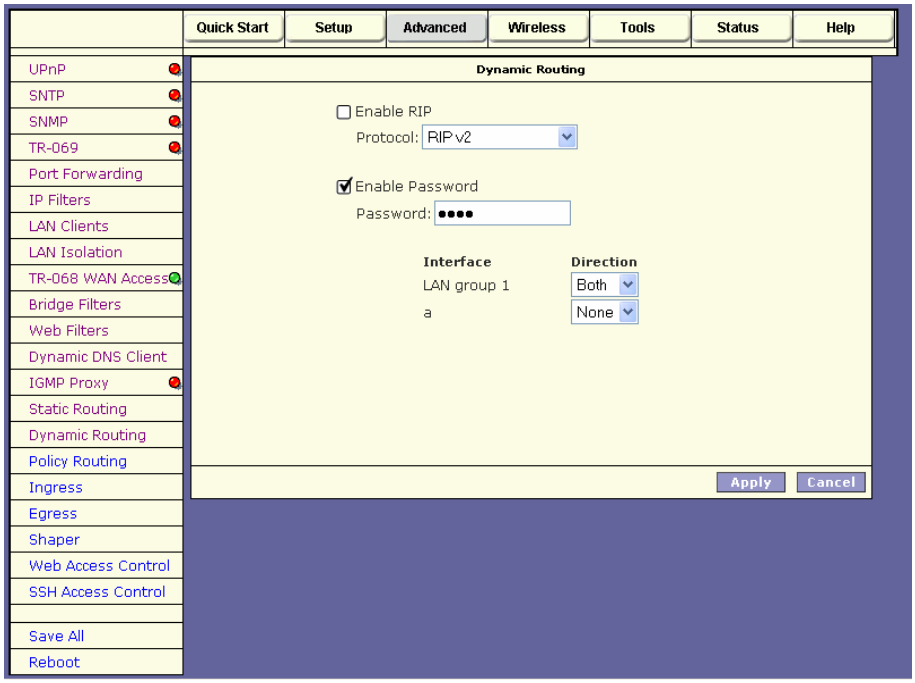
Gateway: The IP address of the next hop through which traffic will flow towards the *destination* subnet.

Metric: Defines the number of hops the between network nodes that data packets travel. *The* default value is *0*, which means that the subnet is directly one hop away on the local LAN network.

Click ***Apply*** to complete the setup. Click ***Save All*** to save the changes.

Dynamic Routing

The dynamic routing feature enables the RG to dynamically define routes for WAN and LAN subnets. Dynamic routing uses routing information protocol (RIP) for exchanging routing information with other routers in the network. It is supported across both WAN and LAN interfaces. Any RIP-enabled router sends out automatic update packets containing its own routing table on a periodic basis (every 30 secs). Similarly, it accepts such periodic updates from other routers and adds, deletes, or modifies routes in its own routing table accordingly. The router is also expected to receive requests for its routing table and respond accordingly. Use the **Dynamic Routing** page to define dynamic routing routes for the available interfaces.



Enable RIP: Enables/disables RIP.

Protocol: The following three RIP versions are available:

- RIP v1 (UDP protocol)
- RIP v2 (multicast protocol)
- RIP v1 compatible (UDP protocol with multicast format)

Note: Routers using RIP v1 or RIP v1-compatible protocol can talk to each other, but not to routers using RIP v2 protocol.

Enable Password: This is an optional field. RIP version v2 compatibility allows you to provide simple plain-text password-based authentication to RIP packets. This field is disabled if RIP v1 protocol is selected.

Password: The password can be up to 16 characters long.

Direction: Normally when RIP is enabled on a router, it dynamically learns/provides routes on all its configured interfaces. This parameter allows you to select the interfaces on which RIP is expected to learn and distribute routing information.

This feature allows you to control how and which routes get distributed through the network. For example, by selecting *In only* mode, routes to private LAN networks are prevented from being sent over to the WAN-side router. The following four direction options are available:

• **Both**: Receive updates on the interface and also send its routing table to other routers connected to that interface.

• **In**: Receive routing updates from other routers connected to that interface but do **NOT** send routing updates on that interface.

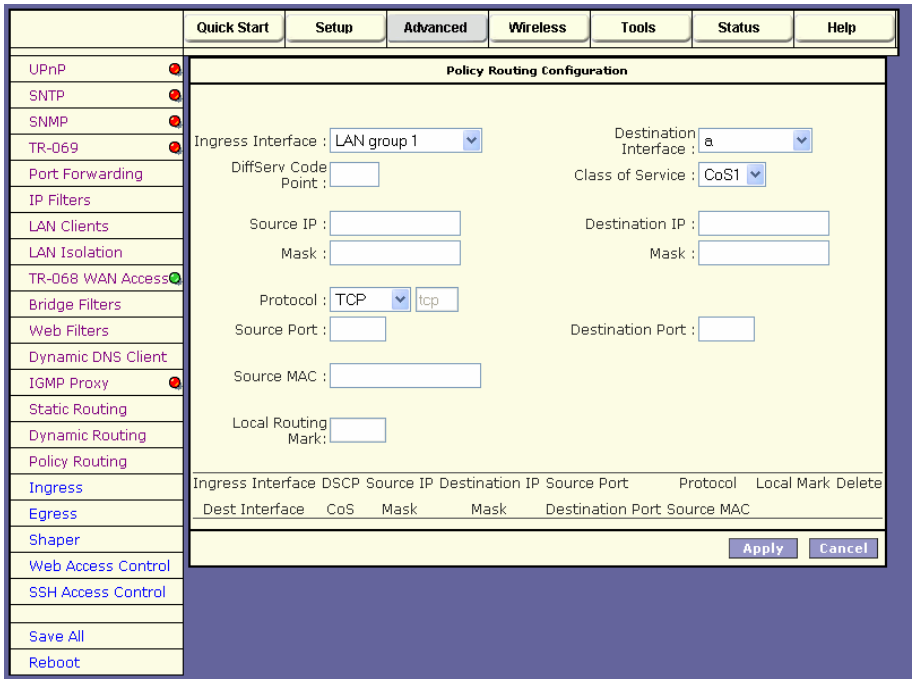
• **Out**: Send routing updates but do **NOT** receive updates on this interface from the other routers connected to that interface.

• **None**: Ignore this interface and do not send or receive routing updates through this interface.

Click ***Apply*** to complete the setup. Click ***Save All*** to save the changes.

Policy Routing

The Policy Routing Configuration page is accessed by selecting Policy Routing on the Advance home page. This page enables you to configure policy routing and QoS.



Ingress Interface: The incoming traffic interface for a Policy Routing rule. Selections include LAN interfaces, WAN interfaces, locally generated (traffic), and not applicable. Examples of Locally generated traffic are: voice packets, packets generated by applications such as DNS, DHCP, etc.

Destination Interface: The outgoing traffic interfaces for a Policy Routing rule. Selections include LAN Interfaces and WAN interfaces.

DiffServ Code Point: The diffServ code point (DSCP) field value ranges from 1 to 255. This field cannot be configured alone; additional fields like IP, Source MAC, and/or Ingress Interface should be configured.

Class of Service: The selections are (in the order of priority): CoS1, CoS2, CoS3, CoS4, CoS5, CoS6, and N/A.

Source IP: The IP address of the traffic source.

Mask: The source IP netmask. This field is required if the source IP has been entered.

Destination IP: The IP address of the traffic destination.

Mask: The netmask of the destination. This field is required if the destination IP has been entered***.***

Protocol: The selections are TCP, UDP, ICMP, Specify, and none. If you choose Specify, you need to enter the protocol number in the box next to the Protocol field. This field cannot be configured alone; additional fields like IP, Source MAC, and/or Ingress Interface should be configured. This field is also required if the source port or destination port has been entered.

Source Port: The source protocol port. You cannot configure this field without

entering the protocol first.

Destination Port: The destination protocol port or port range. You cannot configure this field without entering the protocol first.

Source MAC: The MAC address of the traffic source.

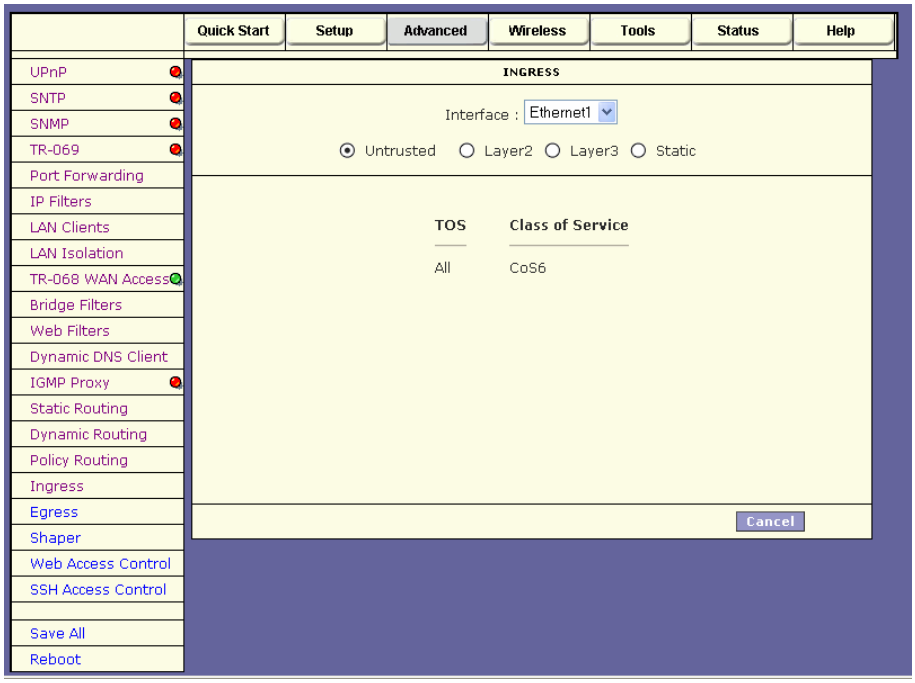
Local Routing Mark: This field is enabled only when Locally Generated is selected in the Ingress Interface field. The mark for DNS traffic generated by different applications is described below:

- Dynamic DNS: 0xE1
- Dynamic Proxy: 0xE2
- Web Server: 0xE3
- MSNTP: 0xE4
- DHCP Server: 0xE5
- IPtables Utility: 0xE6
- PPP Deamon: 0xE7
- IP Route: 0xE8
- ATM Library: 0xE9
- NET Tools: 0xEA
- RIP: 0xEB
- RIP v2: 0xEC
- UPNP: 0xEE
- Busybox Utility: 0xEF
- Configuration Manager: 0xF0
- DropBear Utility: 0xF1
- Voice: 0

Click ***Apply*** to complete the setup. Click ***Save All*** to save the changes.

Ingress

The Ingress page enables you to configure QoS for packets as soon as they come into the RG. This page is accessed by selecting Ingress on the Advance main page.



Interface: For both WAN and LAN interfaces, you can configure QoS for layer 3 (IP) data traffic.

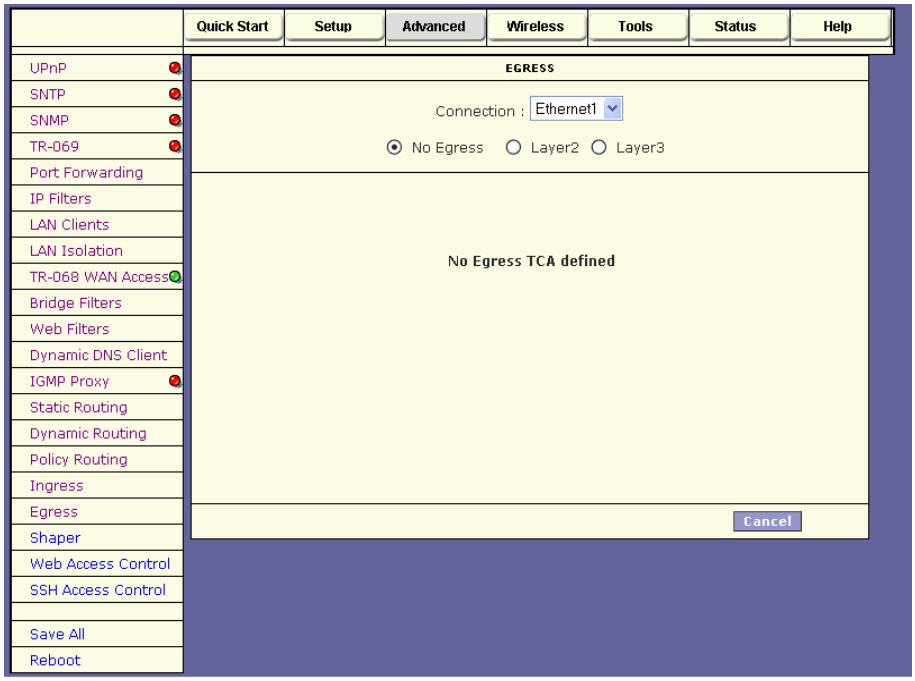
Class of Service: This CoS field allows you to map incoming layer 3 WAN/LAN packets to one of the following CoS (in the order of descending priority): CoS1, CoS2, CoS3, CoS4, CoS5, and CoS6.

ToS: The type of service field takes values from 0 to 255***.***

Click ***Apply*** to complete the setup. Click ***Save All*** to save the changes.

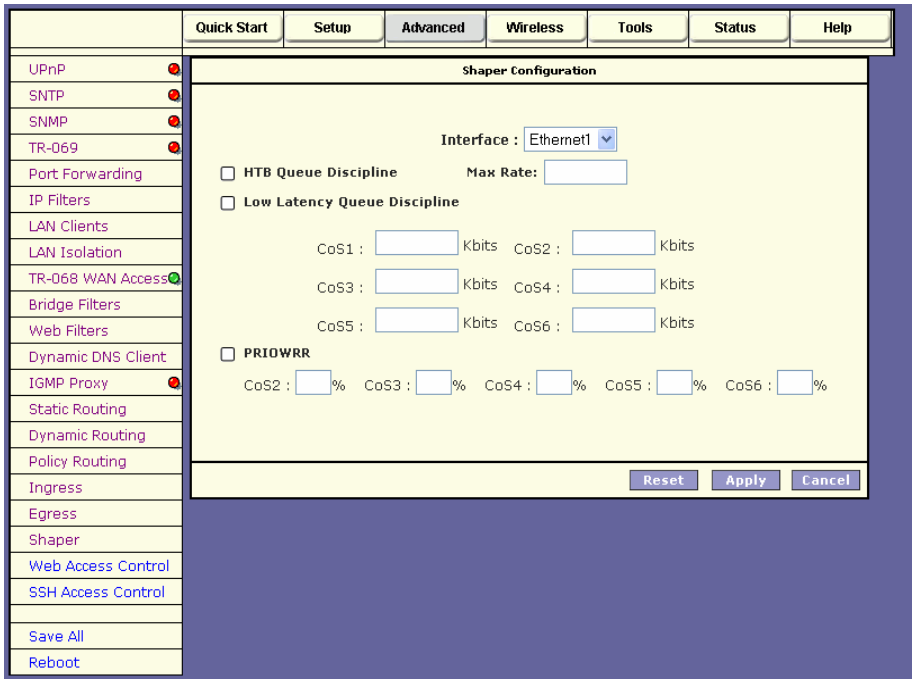
Egress

The default Egress page setting for all interfaces is No Egress. In this mode, the domain mappings of the packets are untouched.



Shaper

The Shaper Configuration page is accessed by selecting Shaper on the Advance main page.



Interface: The selections are WAN/LAN interfaces except WLAN, which does not support Shaper feature. This field needs to be selected before shaper configuration.

Max Rate: This field is applicable for the HTB Queue Discipline and Low Latency Queue Discipline; both are rate-based shaping algorithms.

HTB Queue Discipline: The hierarchical token bucket queue discipline is a rate-based shaping algorithm. This algorithm rate shapes the traffic of a class over a specific interface. All CoSx traffic is assigned a specific rate to which data will be shaped to. For example: If CoS1 is configured to 100Kbps then even if 300Kbps of CoS1 data is being transmitted to the interface only 100Kbps will be sent out.

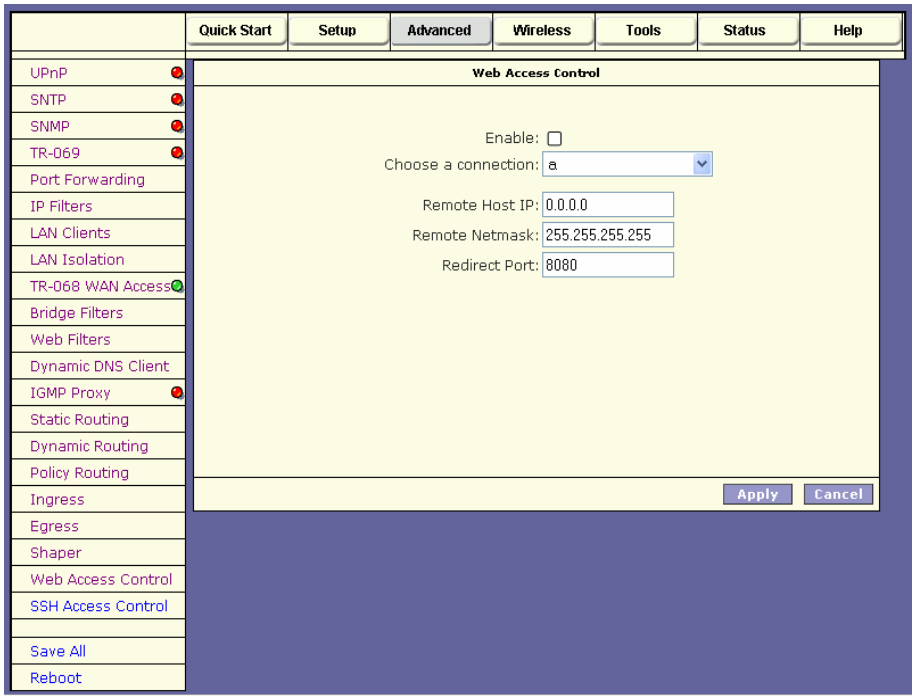
Low Latency Queue Discipline: This is similar to the above algorithm except that CoS1 is not rate limited. So in the example above CoS1 data is not rate limited to 100Kbps but instead all 300Kbps is transmitted. The side effect is that a miss configured stream can potentially take all bandwidth.

PRIOWRR: This is a priority based weighted round robin algorithm operating on CoS2-CoS6. CoS1 queues have the highest priority and are not controlled by the WRR algorithm.

Click ***Apply*** to complete the setup. Click ***Save All*** to save the changes.

Web Access Control

The Web Access Control page allows you to access the RG remotely via the web from the WAN side.



Enable: Enables/disables the remote web access feature.

Choose a Connection: Select the WAN connect over which the remote web access feature is enabled.

Remote Host IP: Enter the IP address of the remote host.

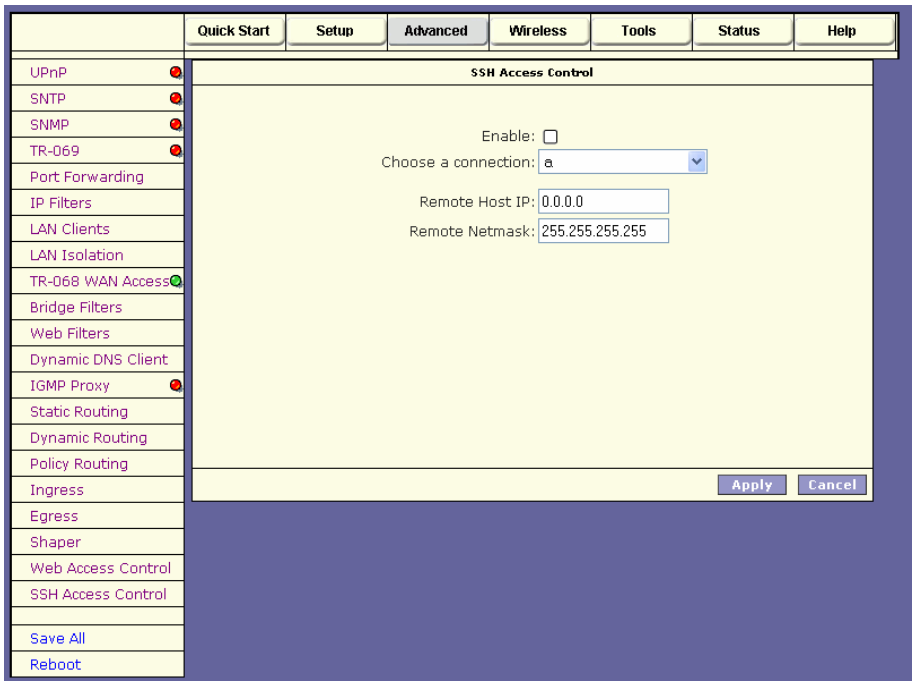
Remote Netmask: Enter the netmask of the remote host.

Redirect Port: You can enter a port number in this field that is different from the well-known IP port number 80. The port number that you enter will be viewed externally and mapped to port 80 internally in the RG.

Click ***Apply*** to complete the setup. Click ***Save All*** to save the changes.

SSH Access Control

The SSH Access Control page allows you to access the RG remotely via SSH from the WAN side.



Enable: Enables/disables the remote web access feature.

Choose a Connection: Select the WAN connect over which the remote web access feature is enabled.

Remote Host IP: Enter the IP address of the remote host.

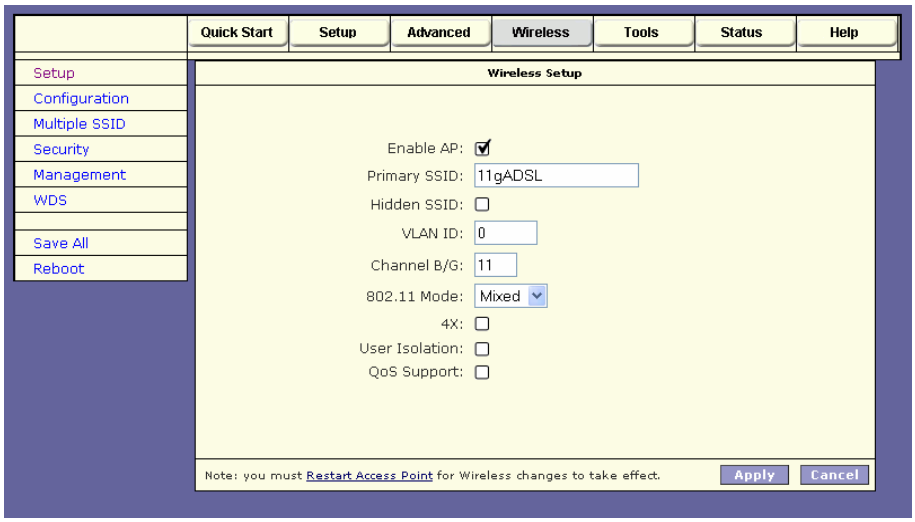
Remote Netmask: Enter the netmask of the remote host.

Click ***Apply*** to complete the setup. Click ***Save All*** to save the changes.

WIRELESS

Setup

This page allow you to enable and disable the wireless LAN function, create a SSID, and select the channel for wireless communications..



***Primary SSID*:** Type an SSID in the text box. The SSID of any wireless device must match the SSID typed here in order for the wireless device to access the LAN and WAN via the router

Hidden SSID: Enables/disables the hidden SSID feature. When hidden SSID is enabled, the SSID is removed from the beacon frames the AP transmits, thus the AP will not be seen by any other station.

VLAN ID: The VLAN ID for the primary SSID. By default, multiple SSID is disabled and the VLAN ID of the primary SSID is *0*. When you enable multiple SSID, you are prompted to change the VLAN ID of the primary SSID to a unique value between *1 - 4095*.

***Channel B/G*:** The channel on which the AP and the wireless stations communicate. Different domains have different ranges of channels. For FCC in 2.4 GHz, the default channel is 11

802.11 Mode: Select mode from the dropping list. (Mixed/ b/ b+/ 11g only)

4X: Enables/disables the 4x feature for 802.11g mode. This function is TI proprietary and is only available when both TI wireless station card and TI RG are used.

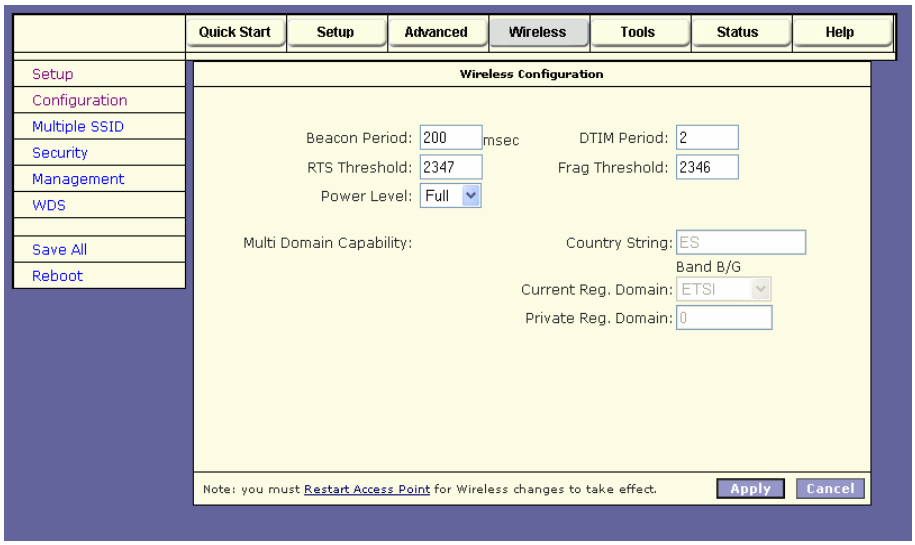
User Isolation: When checked, wireless users will not be able to directly access other wireless users.

QoS Support: Enable or Disable this function.

Click ***Apply*** to complete the setup. Click ***Save All*** to save the changes.

Configuration

This Wireless Configuration page shows the Wireless Function Status.



Beacon Period: Type the Beacon Period in the text box. You can specify a value from 0 to 65535. The default Beacon Period is 200.

DTIM Period: Type a DTIM (Delivery Traffic Indication Message) Period in the text box. You can specify a value between 1 and 255. The default value is 2.

RTS Threshold: Type the RTS (Request-To-Send) threshold in the text box. You can specify a value from 0 to 4096. The default value is 2347.

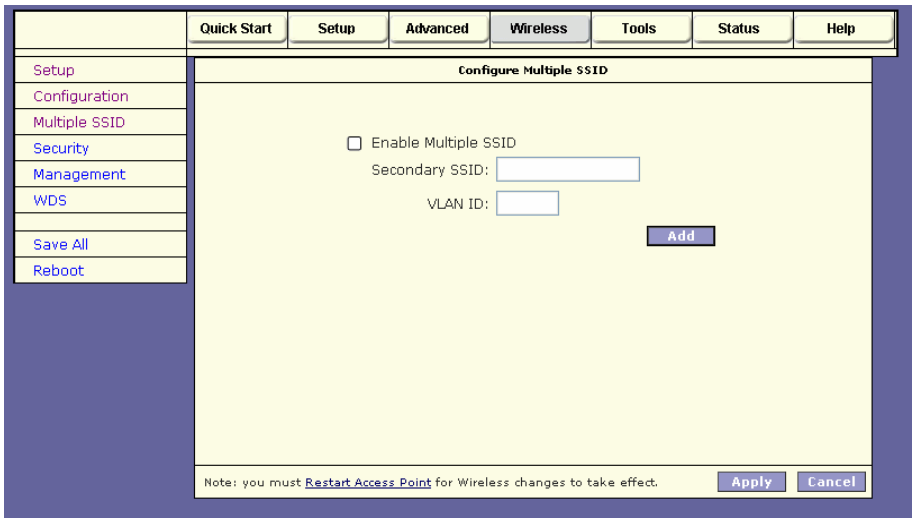
Frag Threshold: Type the fragmentation in the text box. You can specify a value from 0 to 4096. The default value is 2346.

Power Level: Adjust the power of the antenna transmission by selecting from the dropping list.

Click ***Apply*** to complete the setup. Click ***Save All*** to save the changes.

Multiple SSID

You can access the Multiple SSID page by clicking the Multiple SSID link. The Enable SSID field allows you to create multiple SSIDs for the Wireless Router.



Enable Multiple SSID: Enables/disables multiple SSID.

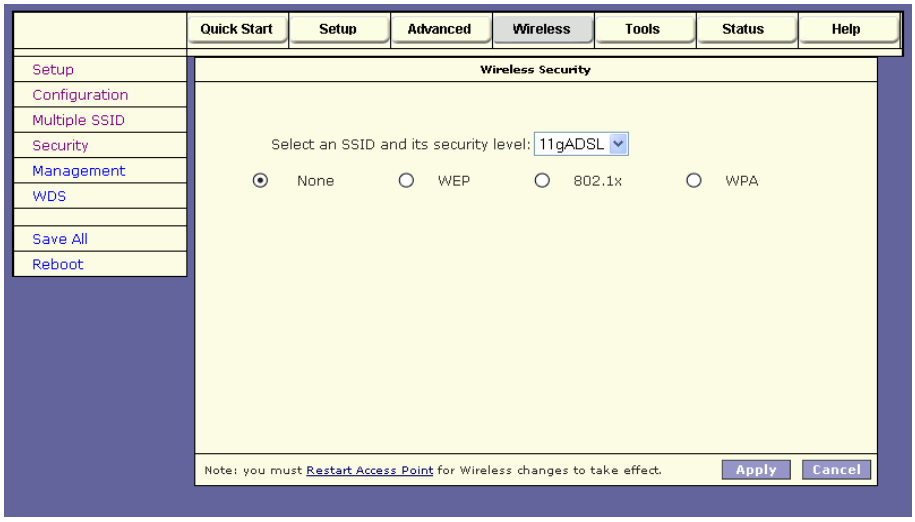
Secondary SSID: The secondary SSID of the Wireless Router is up to 32 characters and is unique from the primary SSID.

VLAN ID: The VLAN ID of the secondary SSID, which has a unique value between 1 - 4095.

Click ***Apply*** to complete the setup. Click ***Save All*** to save the changes.

Security

Select a Wireless Security level



None: Disable Wireless encryption.

WEP: WEP encryption scrambles the data transmitted between the wireless stations and the access points to keep network communications private. It encrypts uni-cast and multicast communications in a network. Both the wireless stations and the access points must use the same WEP key for data encryption and decryption.

802.1x: The IEEE 802.1x standards outline enhanced security methods for both the authentication of wireless stations and encryption key management.

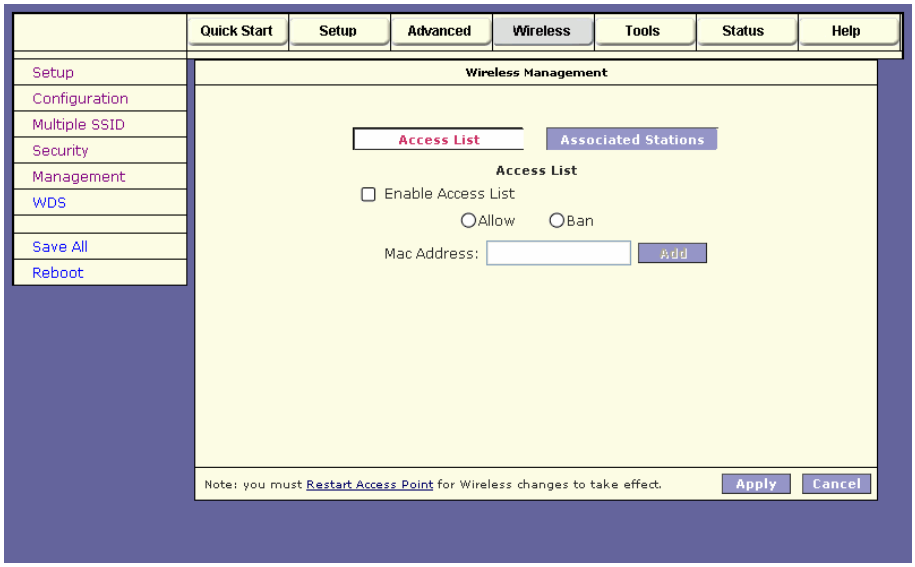
WPA: Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i security specification draft. Key differences between WPA and WEP are user authentication and improved data encryption.

WPA2: WPA2, also known as 802.11i, uses advanced encryption standard counter mode CBC-MAC protocol (AES-CCMP) for data encryption.
Enable stations with WPA2 capability to connect the AP. This option is available under the WPA option.

Click ***Apply*** to complete the setup. Click ***Save All*** to save the changes.

Management

The Wireless Management page allows your prestige can check the MAC addresses of Wireless stations against a list of allowed or denied MAC addresses.



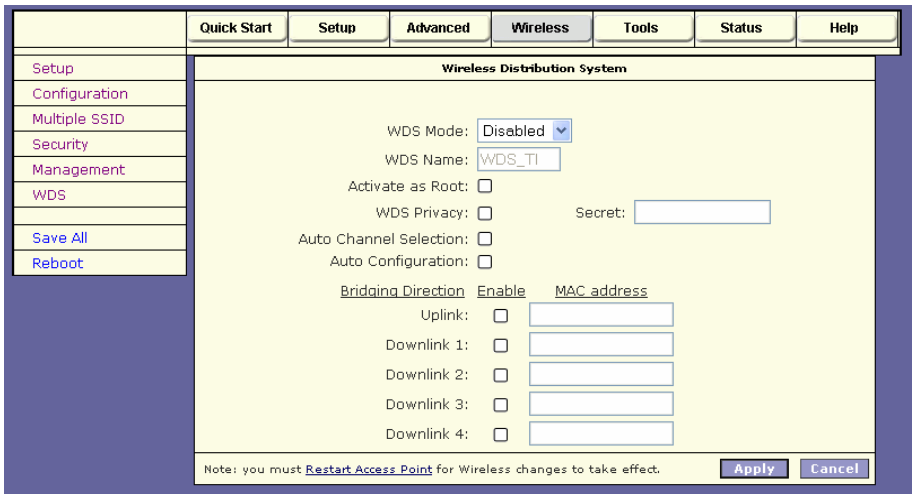
MAC Address: Enter the MAC Address. (Format: 00-0e-2e-41-23-4e). Access List can accept 64 groups.

Enable Access List: Enable the Wireless Management by Access List.

Click ***Apply*** to complete the setup. Click ***Save All*** to save the changes.

WDS

Wireless distribution system (WDS) is a system that interconnects BSS to build a premise wide network. WDS network allows users of mobile equipment to roam and stay connected to the available network resources. You can configure your Wireless Router as WDS mode using the WDS page.



WDS Mode:

Bridge: In Bridge mode, the Wireless Router basic service set (BSS) service is enabled.

Repeater: In Repeater mode, the Wireless Router BSS is disabled when connection to the upper layer Wireless Router is established.

Crude: In Crude mode, the Wireless Router BSS service is always enabled; however, the links between APs are configured statically and are not maintained.

Disabled(Default): WDS inactive.

In Both Bridge and Repeater modes, WDS uses management protocol to establish and maintain links between APs.

WDS Name: The WDS name is used to identify WDS network. The field takes up to eight characters. Two or more WDS networks may exist in the same area.

Activate as Root: This field must be checked for the root device in WDS hierarchy. Only one WDS root device may exist in WDS network. This field is not applicable for Crude mode.

WDS Privacy: Checking this field commands WDS manager to use a secured connection between APs in the WDS network. Security settings must be the same in all APs in the WDS network.

Note: WDS privacy is not supported in Crude mode.

Secret: The 32-character alpha-numeric privacy key.

Auto Channel Selection: Auto channel selection is not supported in the current version.

Auto Configuration: Auto configuration is not supported in the current version.

Uplink Connection Check Box: The BSS ID of the upper device in the WDS

hierarchy. This uplink cannot be configured if Root is enabled.

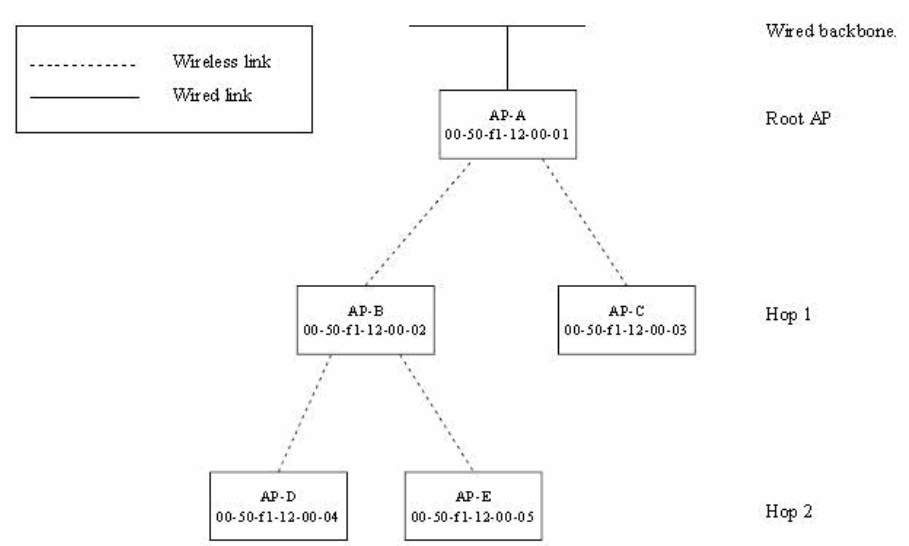
Downlink Connection Check Boxes: The BSS ID of the lower device in the WDS hierarchy connected to this Wireless Router. Up to four downlinks can be configured.

Click ***Apply*** to complete the setup. Click ***Save All*** to save the changes.

How to setting up the WDS with NSP?

Reference doc: AP-DK_6_3_AN_WDS_v1_0.pdf and

Environment:



Test case:

Please reference my statement as following:

PC-A(192.168.1.30)←wired→AR7WRD(AP-A)←wireless→AR7WRD(AP-B)←wired →PC-B(192.168.1.55)

When you enabled WDS function success then you can ping from PC-A to PC-B.

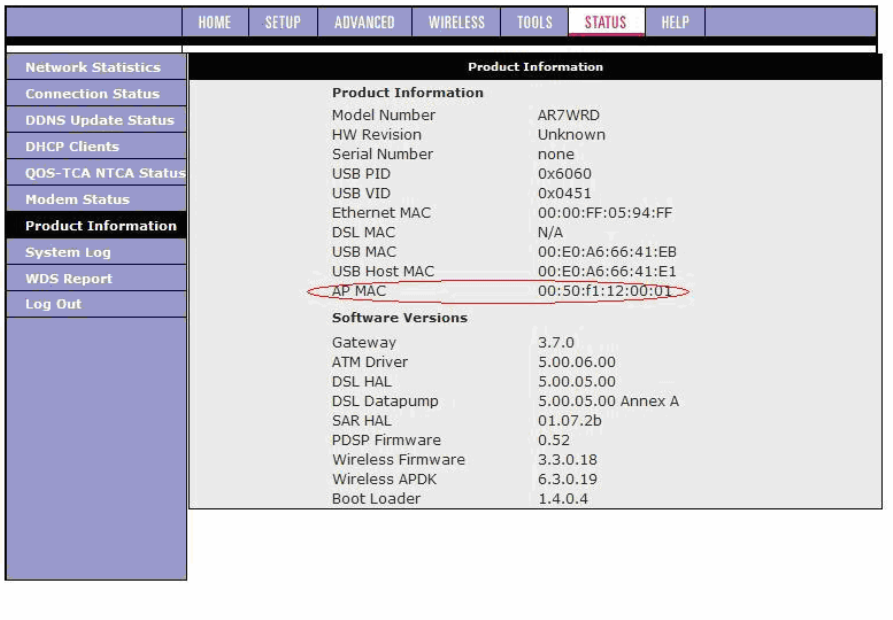
NSP Setting procedure,

1. Make sure you set up the WLAN MAC address at our boot loader.

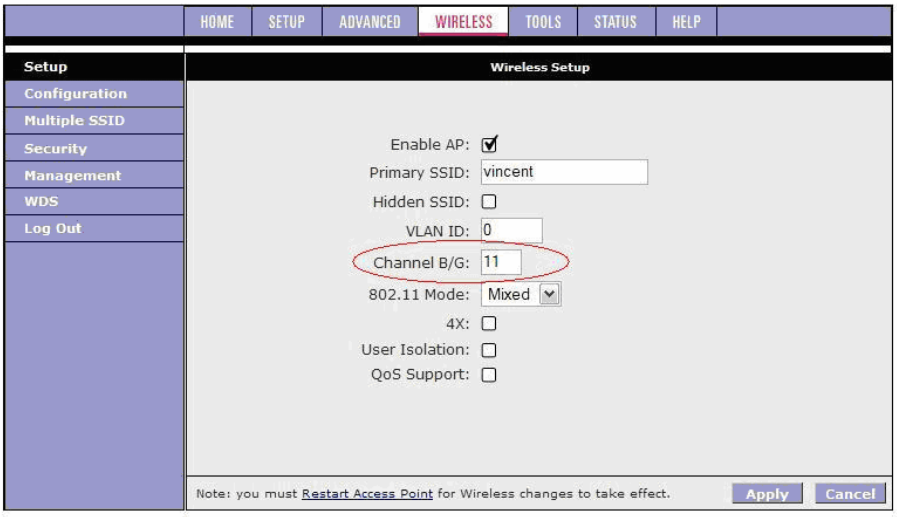
   Example:

```
WLAN_EEPROM6    01B701013900001100040101010005010600020102010210E000A000205020411
WLAN_EEPROM7    22440306102030313240040954492041435831303005075449205465737401 08
WLAN_EEPROM8    273047D16293218E0502000037006F00A500E100040444100E0045100100185A
WLAN_EEPROM9    4000145A1E00020E0801D7000A0105034600A40185095000FE000A01DD035000
WLAN_EEPROM10   EF0185090107100000400000010000050400010100000000FFFFFFFFFDFDFDFD
WLAN_EEPROM11   FBF1F1F1F10E04FCFCFCFDFFFFFFFE090000FF090909FF090909090909090909
WLAN_EEPROM12   09090909090909090000009FFFFFFFEFCFCFCFD09090909090909090909090E
WLAN_EEPROM13   0100000000000000000000000000000302A318A31807000120000000000000000
WLAN_EEPROM14   00000000000000000000000000000000000000000000000000000000000000
NVS_TFTP_LOAD   0
connection0     0xcd0b

apBridgeMode    1
mtd1    0x90020090,0x9009e000
mtd0    0x9009e000,0x90400000
modulation      0xff
connection1     0x9817

WLAN_HWADDR     00:50:f1:12:00:01
#
```

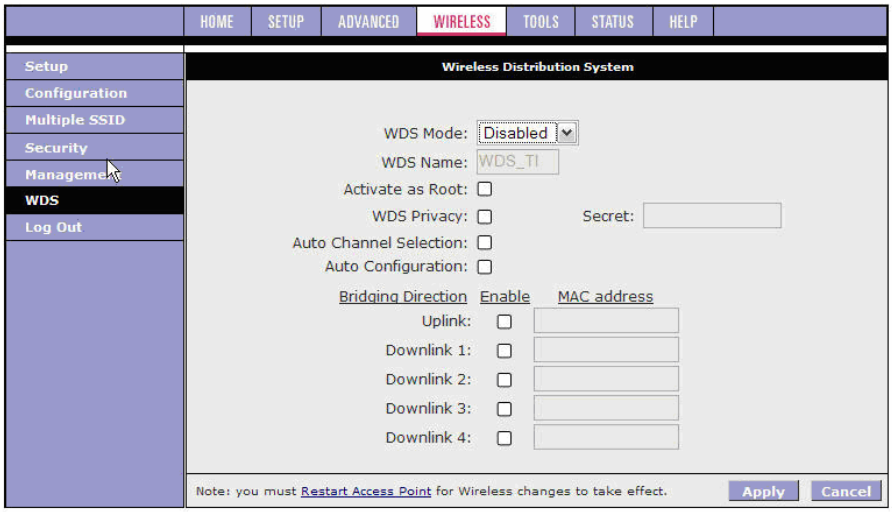
2. Please check your AR7WRD's MAC address at web
   Example:



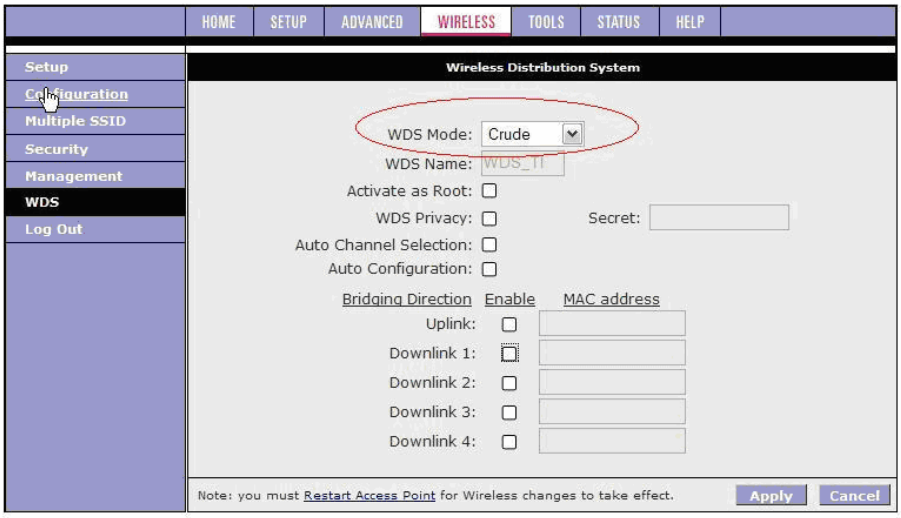
3. Please check your AP at the same channel, make sure AP-A and AP-B at the same channel,
   Example:



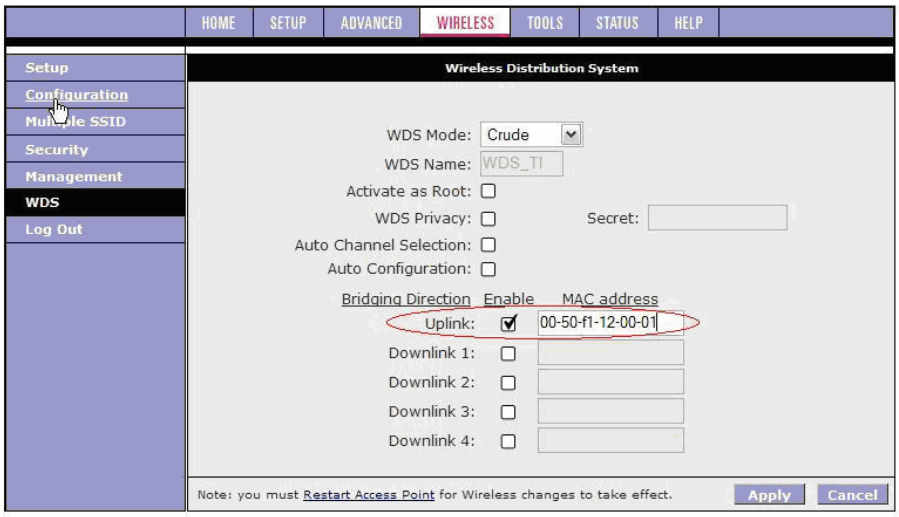
4. Click the wireless at top bar and click the WDS at left bar and you will see the screen as following.
   Example:



5. Select the WDS mode to Crude mode.
   Example:



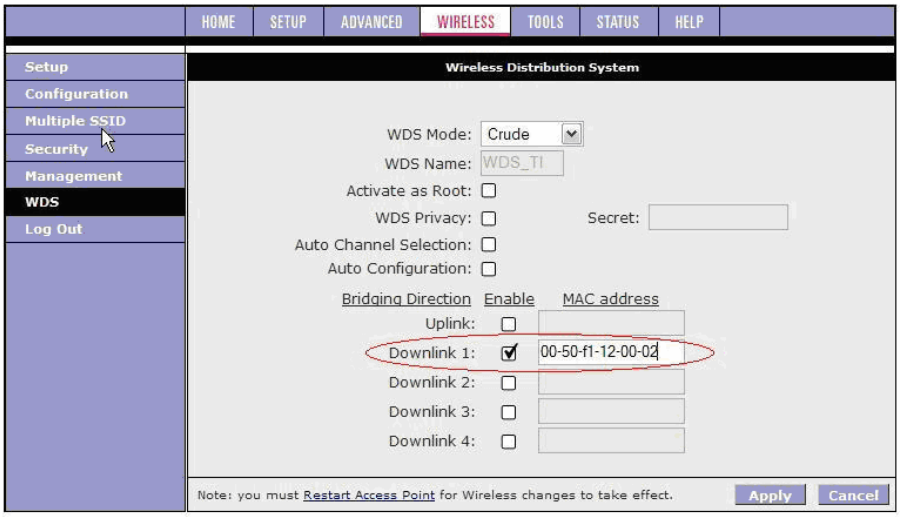
6. Fill in the up-link blanks with AP-B's MAC address at AP-A's WDS web screen as following.
   Example:



7. Fill in the down-link blanks with AP-A's MAC address at AP-B's WDS web screen

as following.

Example:



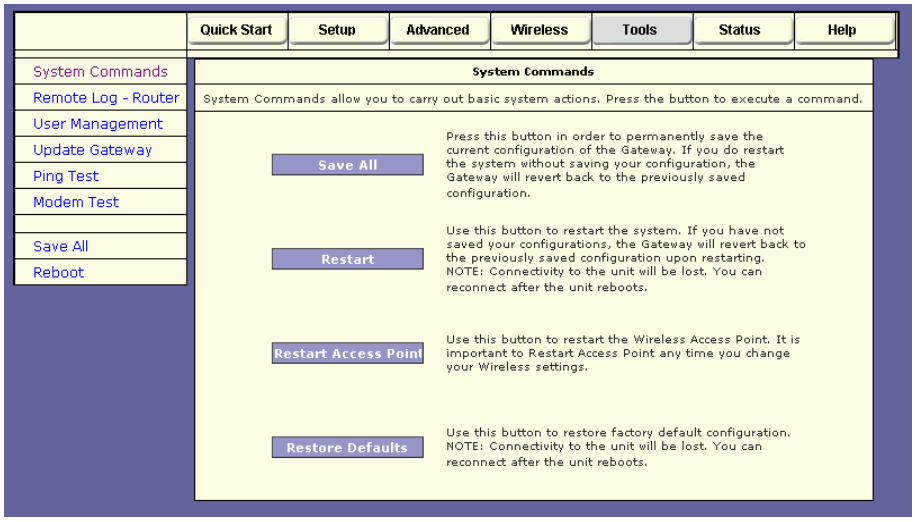
8. Click on the TOOLS at top bar and select the System Commands at left bar and then click on the SAVE ALL and Restart.
9. You can ping the PC each other.

TOOLS

The Tools section allows you to save the configuration, restart the gateway, update the gateway firmware, setup user and remote log information and run Ping and Modem tests.

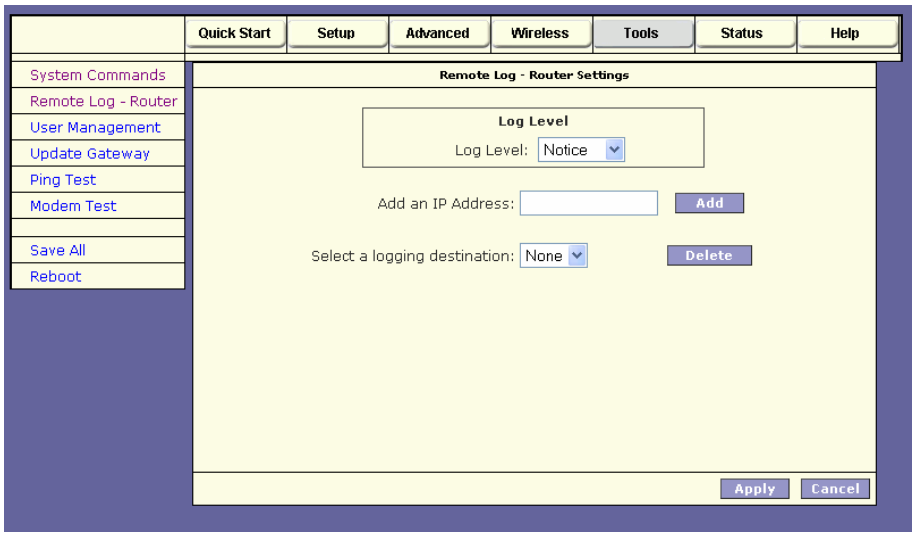
System Commands

System Commands allow you to carry out basic system actions, Press the button to execute a command.


Quick Start
Setup
Advanced
Wireless
Tools
Status
Help
System Commands
Remote Log - Router
User Management
Update Gateway
Ping Test
Modem Test
Save All
Reboot
System Commands
System Commands allow you to carry out basic system actions. Press the button to execute a command.
Save All
Press this button in order to permanently save the current configuration of the Gateway. If you do restart the system without saving your configuration, the Gateway will revert back to the previously saved configuration.
Restart
Use this button to restart the system. If you have not saved your configurations, the Gateway will revert back to the previously saved configuration upon restarting.
NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Restart Access Point
Use this button to restart the Wireless Access Point. It is important to Restart Access Point any time you change your Wireless settings.
Restore Defaults
Use this button to restore factory default configuration.
NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.

Remote Log

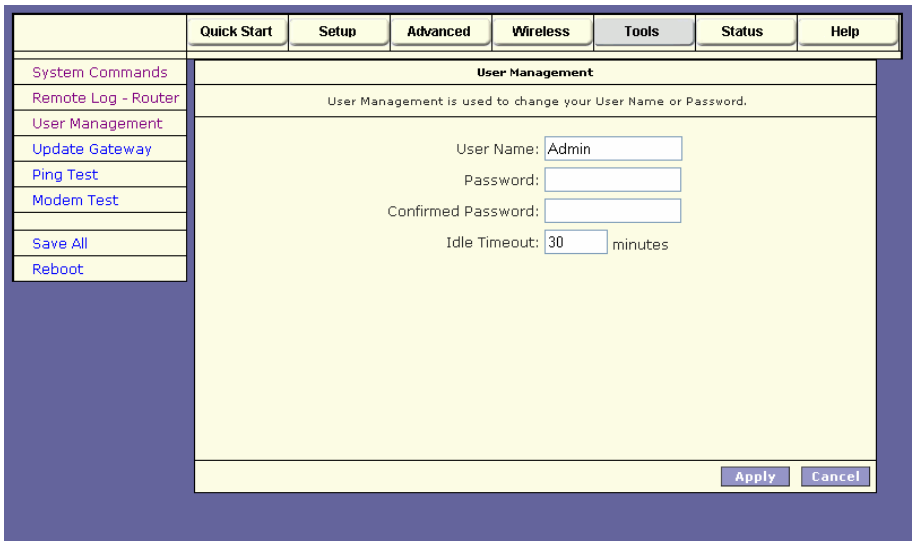
The Router Table page displays routing table and allows the user to manually enter the routing entry. The routing table will display the routing status of Destination, Netmask, Gateway and Interface. The interface br0 means the USB interface; lo0 means the loopback interface and ppp1 means the PPP interface. The Gateway is the learned Gateway.



Click ***Apply*** to complete the setup. Click ***Save All*** to save the changes..

User Management

User Management is used to change your User Name or Password.



User Name: Default is 'Admin'. You can enter your new user name here.

Password: Default is 'Admin'. You can enter your new password here.

Confirmed Password: Enter your new password here again to confirmed.

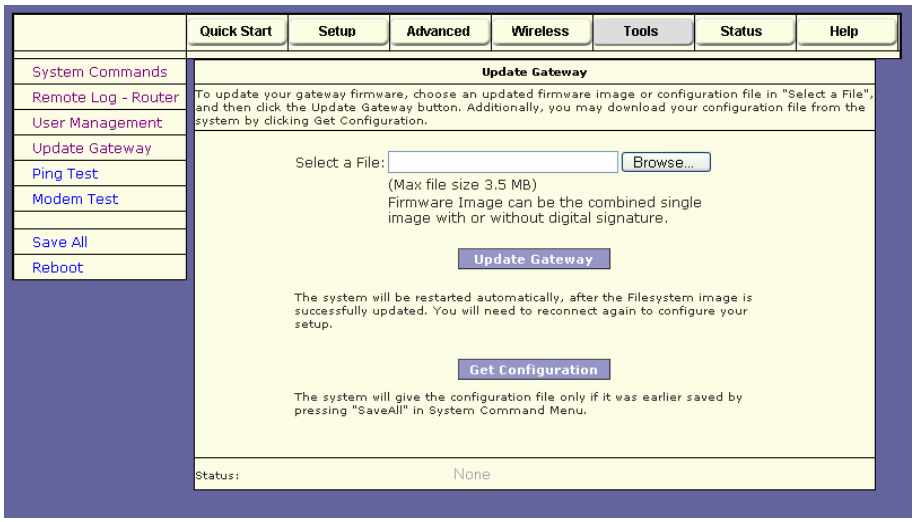
Idle Timeout: The default is *30*minutes. You will need to log back onto the RG after your session has been inactive for 30 minutes. You can change the timeout here.

Click ***Apply*** to complete the setup. Click ***Save All*** to save the changes.

Update Gateway

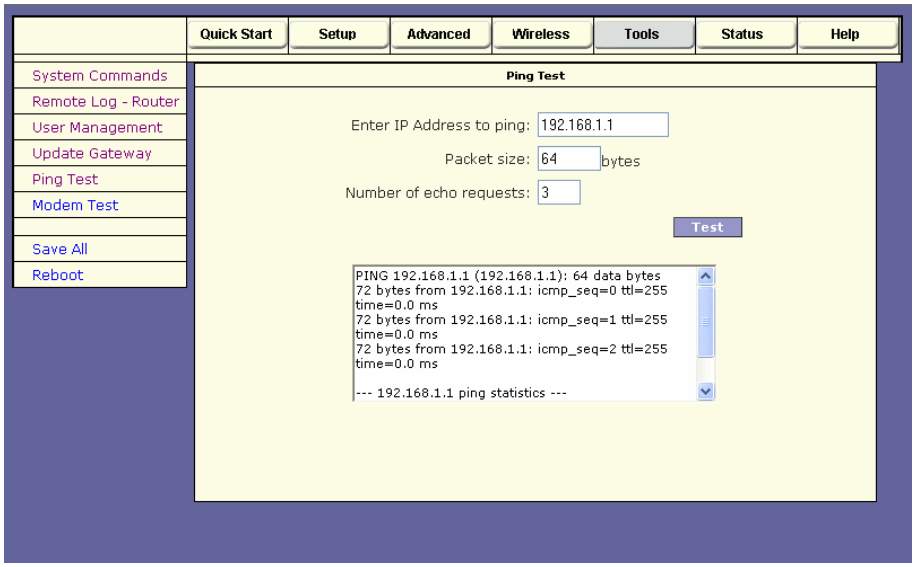
To update your gateway firmware, choose an update image (Kernel/ File system) or configuration file In Select a File, and then click the Update Gateway button.

Additionally, you may download your configuration file from the system by clicking Get Configuration.


Quick Start
Setup
Advanced
Wireless
Tools
Status
Help
System Commands
Remote Log - Router
User Management
Update Gateway
Ping Test
Modem Test
Save All
Reboot
Update Gateway
To update your gateway firmware, choose an updated firmware image or configuration file in "Select a File", and then click the Update Gateway button. Additionally, you may download your configuration file from the system by clicking Get Configuration.
Select a File:
Browse...
(Max file size 3.5 MB)
Firmware Image can be the combined single image with or without digital signature.
Update Gateway
The system will be restarted automatically, after the Filesystem image is successfully updated. You will need to reconnect again to configure your setup.
Get Configuration
The system will give the configuration file only if it was earlier saved by pressing "SaveAll" in System Command Menu.
Status:
None

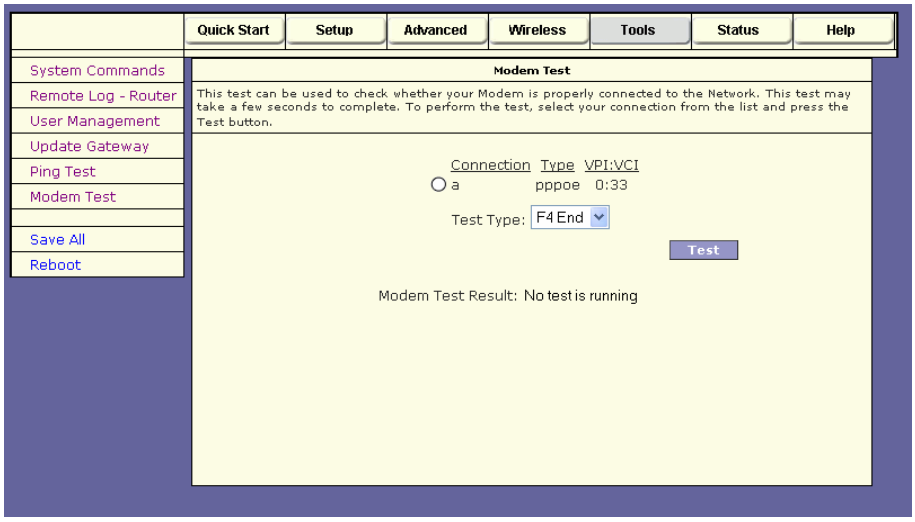
Ping Test

Packet INternet Groper is protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.



Modem Test

The Modem Test page is used to check the connectivity to the WAN. This test may take a few seconds to complete. Before running this test, make sure you have at least one WAN connection configured and have a valid DSL link. If the DSL link is not connected, the test will fail. Also make sure the DSLAM supports this feature. Not all DSLAMs have F4 and F5 support. F4/F5 cells are used for operation, administration, and maintenance (OAM) on ATM level.

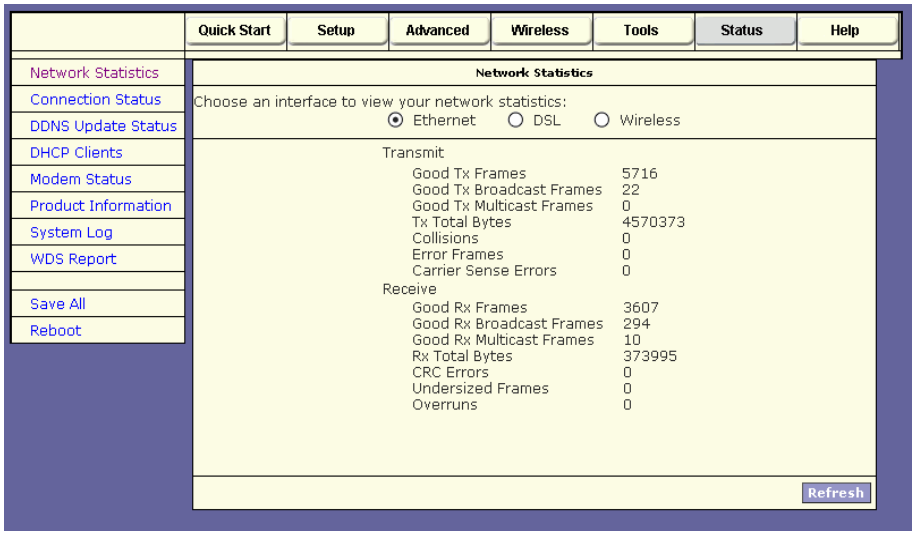


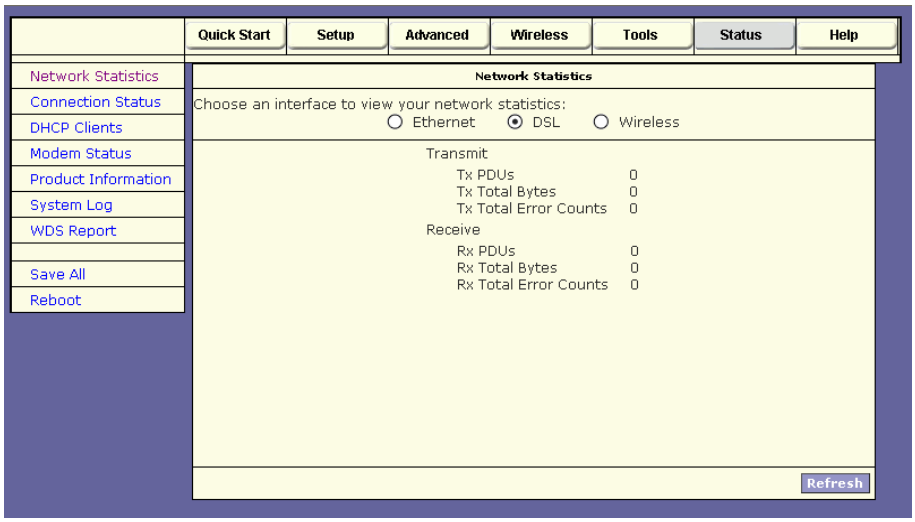
STATUS

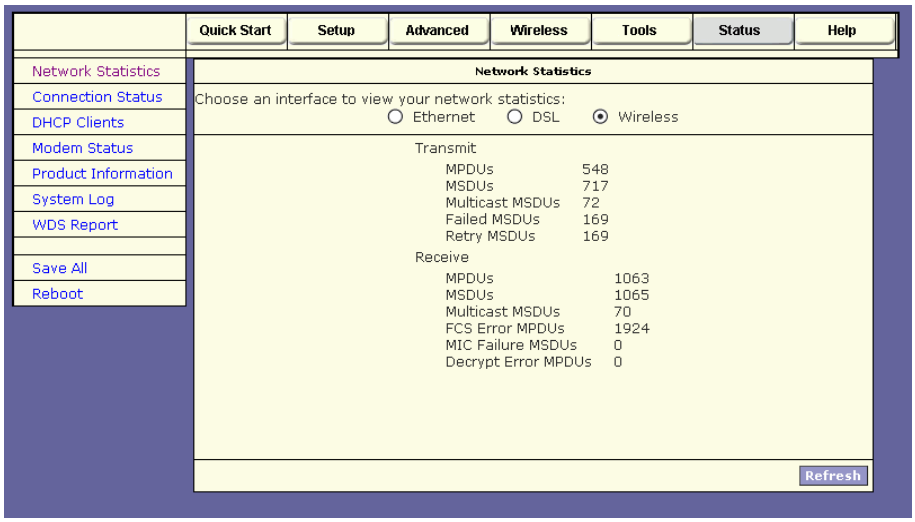
The Status section allows you to view the Status/Statistics of different connections and interfaces.

Network Statistics

The Ethernet Network Statistics page shows the statistics for the Ethernet connection.
The DSL Network Statistics page shows the statistics for the DSL connection.
The Wireless Network Statistics page shows the statistics for the Wireless connection.

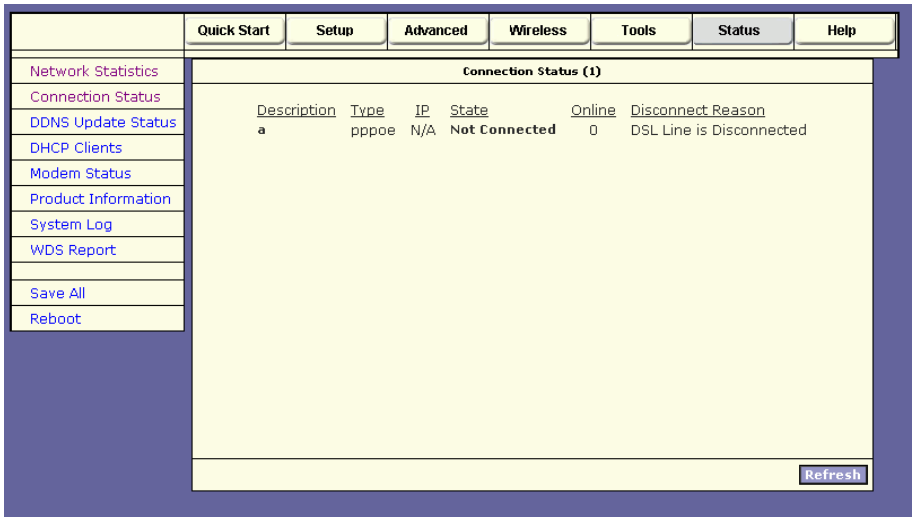





Quick Start
Setup
Advanced
Wireless
Tools
Status
Help
Network Statistics
Connection Status
DHCP Clients
Modem Status
Product Information
System Log
WDS Report
Save All
Reboot
Network Statistics
Choose an interface to view your network statistics:
Ethernet
DSL
Wireless
Transmit
MPDUs 548
MSDUs 717
Multicast MSDUs 72
Failed MSDUs 169
Retry MSDUs 169
Receive
MPDUs 1063
MSDUs 1065
Multicast MSDUs 70
FCS Error MPDUs 1924
MIC Failure MSDUs 0
Decrypt Error MPDUs 0
Refresh

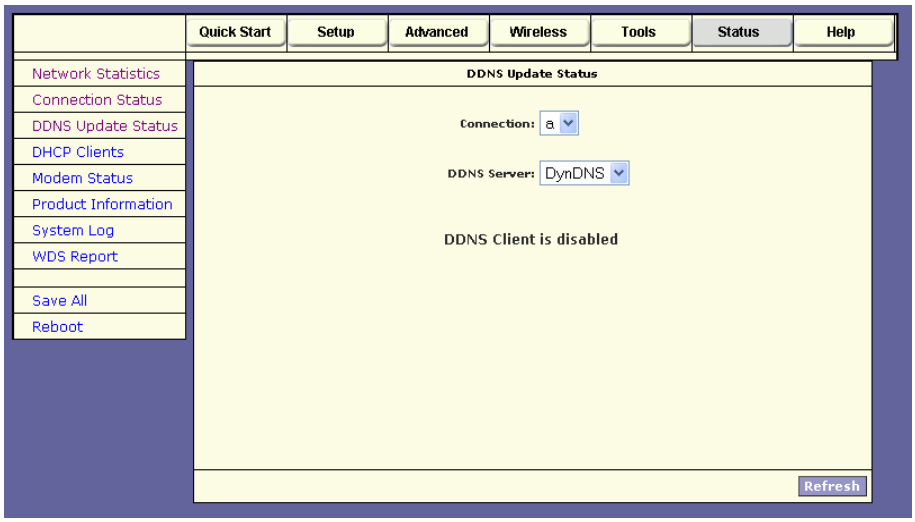
Connection Status

The Connection Status page shows the status of PPP for each PPP interface.



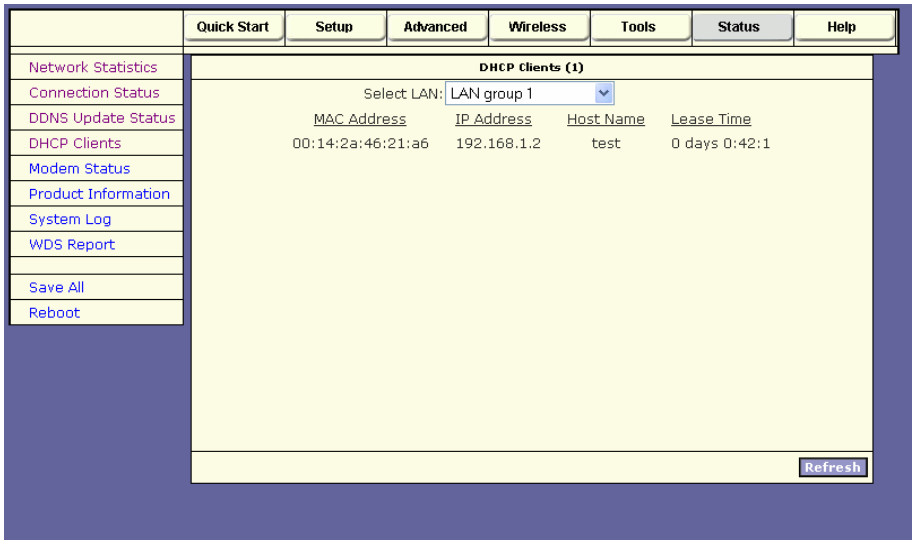
DDNS Update Status

You can view the DDNS update status of your WAN connection from the DDNS Status page.



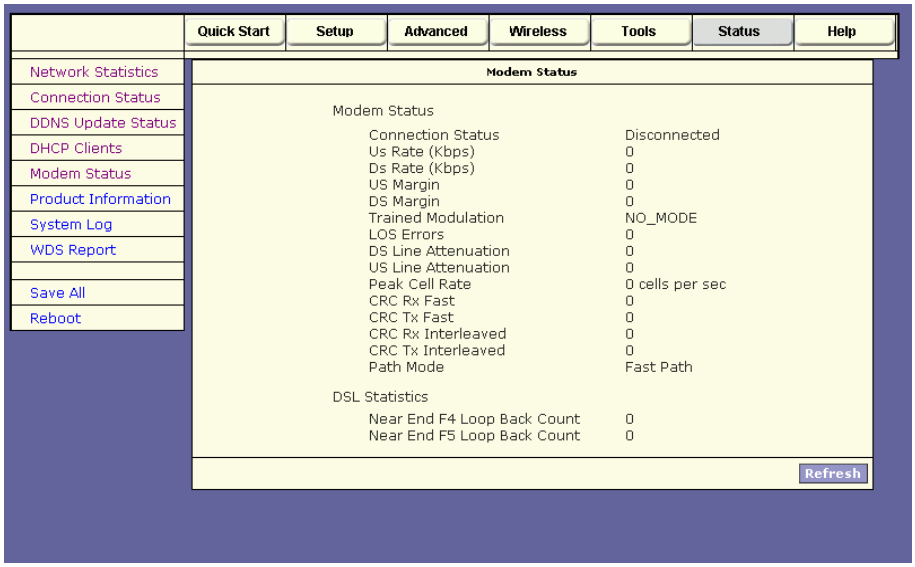
DHCP Clients

The DHCP Clients page shows the MAC Address, IP Address, Host Name and Lease Time.



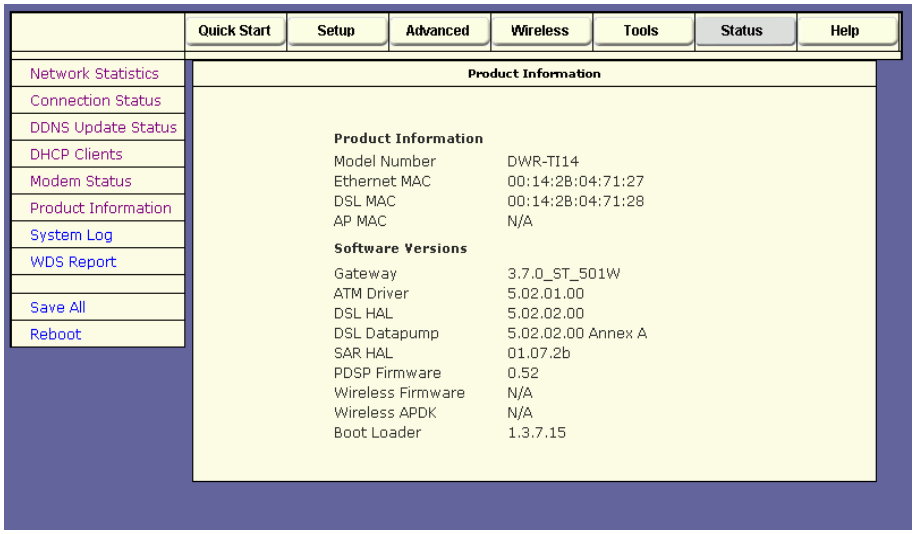
Modem Status

The Modem Status page shows the modem status and DSL statistics.



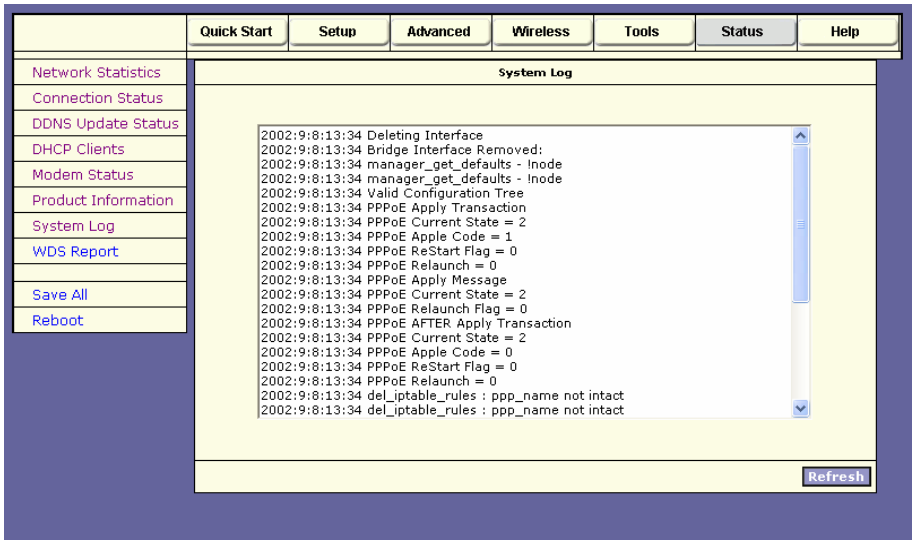
Product Information

The Product Information page shows the product information and software versions.



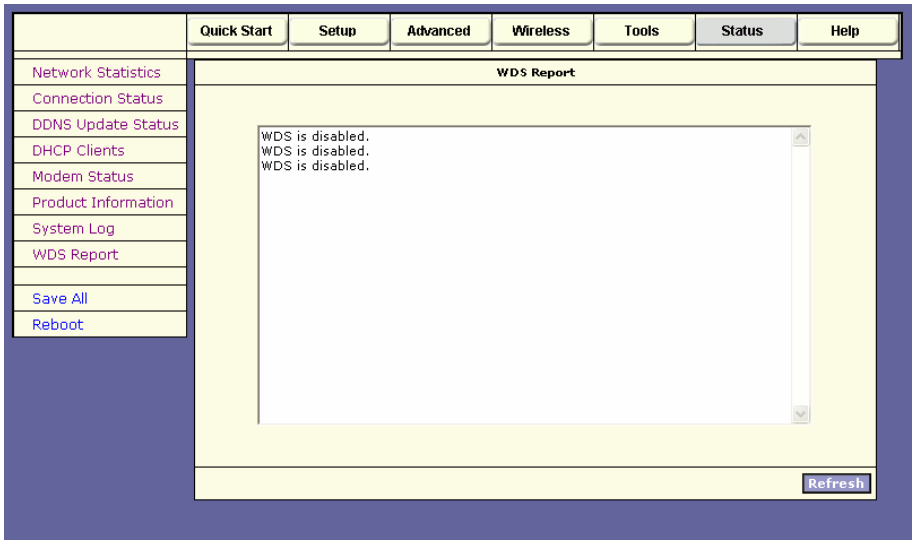
System Log

The System Log page shows the events triggered by the system.



WDS Report

You can view the WDS report for your RG (AP) by clicking the WDS Report link from the Status main page. The WDS Report page allows you to view the following WDS-related wireless activities:



•WDS configuration and states

•WDS management statistics

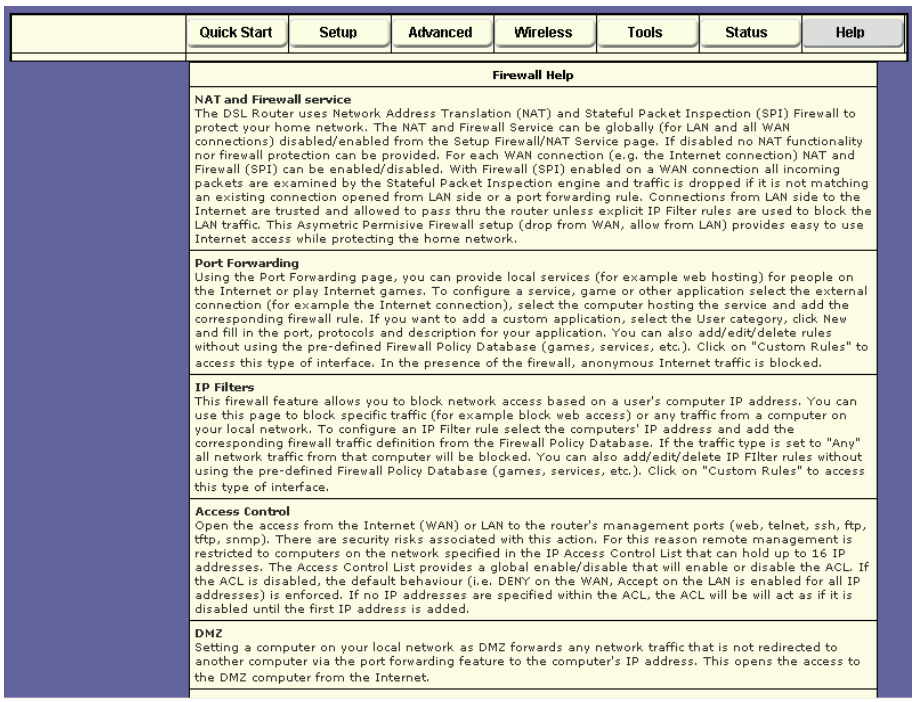
•WDS database

HELP

This section takes you to different Help Sections for Firewall, Bridge Filters, LAN Clients and PPP Connection.

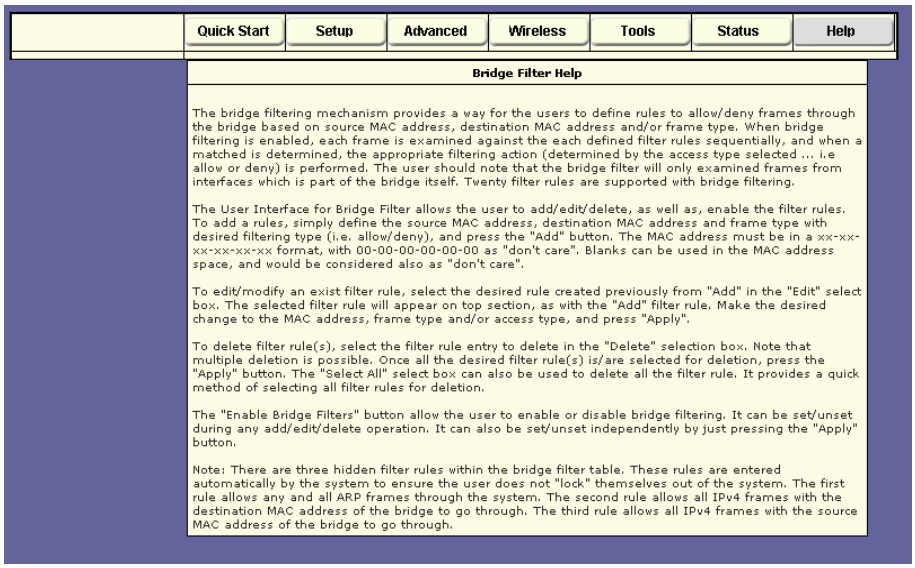
Firewall Help

Help for Port Forwarding, Access Control, and Advanced Security.


Quick Start
Setup
Advanced
Wireless
Tools
Status
Help
Firewall Help
NAT and Firewall service
The DSL Router uses Network Address Translation (NAT) and Stateful Packet Inspection (SPI) Firewall to protect your home network. The NAT and Firewall Service can be globally (for LAN and all WAN connections) disabled/enabled from the Setup Firewall/NAT Service page. If disabled no NAT functionality nor firewall protection can be provided. For each WAN connection (e.g. the Internet connection) NAT and Firewall (SPI) can be enabled/disabled. With Firewall (SPI) enabled on a WAN connection all incoming packets are examined by the Stateful Packet Inspection engine and traffic is dropped if it is not matching an existing connection opened from LAN side or a port forwarding rule. Connections from LAN side to the Internet are trusted and allowed to pass thru the router unless explicit IP Filter rules are used to block the LAN traffic. This Asymetric Permisive Firewall setup (drop from WAN, allow from LAN) provides easy to use Internet access while protecting the home network.
Port Forwarding
Using the Port Forwarding page, you can provide local services (for example web hosting) for people on the Internet or play Internet games. To configure a service, game or other application select the external connection (for example the Internet connection), select the computer hosting the service and add the corresponding firewall rule. If you want to add a custom application, select the User category, click New and fill in the port, protocols and description for your application. You can also add/edit/delete rules without using the pre-defined Firewall Policy Database (games, services, etc.). Click on "Custom Rules" to access this type of interface. In the presence of the firewall, anonymous Internet traffic is blocked.
IP Filters
This firewall feature allows you to block network access based on a user's computer IP address. You can use this page to block specific traffic (for example block web access) or any traffic from a computer on your local network. To configure an IP Filter rule select the computers' IP address and add the corresponding firewall traffic definition from the Firewall Policy Database. If the traffic type is set to "Any" all network traffic from that computer will be blocked. You can also add/edit/delete IP FIlter rules without using the pre-defined Firewall Policy Database (games, services, etc.). Click on "Custom Rules" to access this type of interface.
Access Control
Open the access from the Internet (WAN) or LAN to the router's management ports (web, telnet, ssh, ftp, tftp, snmp). There are security risks associated with this action. For this reason remote management is restricted to computers on the network specified in the IP Access Control List that can hold up to 16 IP addresses. The Access Control List provides a global enable/disable that will enable or disable the ACL. If the ACL is disabled, the default behaviour (i.e. DENY on the WAN, Accept on the LAN is enabled for all IP addresses) is enforced. If no IP addresses are specified within the ACL, the ACL will be will act as if it is disabled until the first IP address is added.
DMZ
Setting a computer on your local network as DMZ forwards any network traffic that is not redirected to another computer via the port forwarding feature to the computer's IP address. This opens the access to the DMZ computer from the Internet.

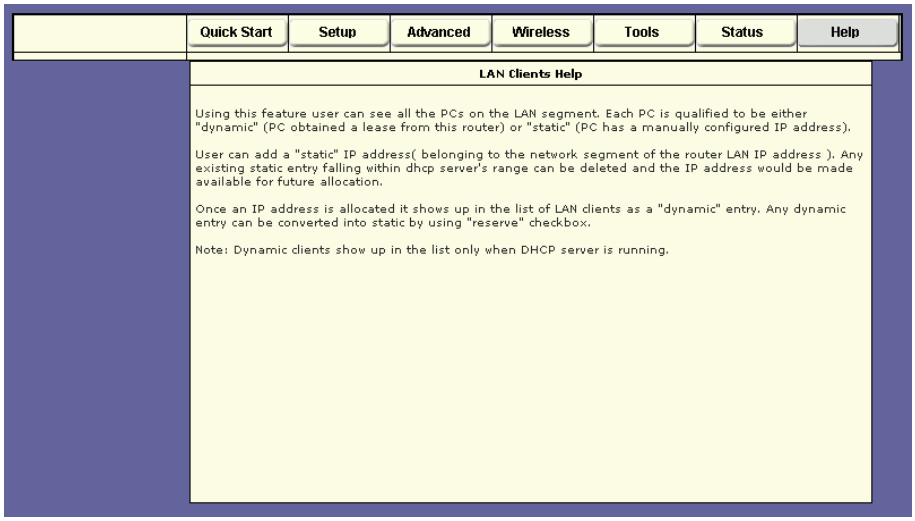
Bridge Filter Help

Help section for Bridge Filters.


Quick Start
Setup
Advanced
Wireless
Tools
Status
Help
Bridge Filter Help
The bridge filtering mechanism provides a way for the users to define rules to allow/deny frames through the bridge based on source MAC address, destination MAC address and/or frame type. When bridge filtering is enabled, each frame is examined against the each defined filter rules sequentially, and when a matched is determined, the appropriate filtering action (determined by the access type selected ... i.e allow or deny) is performed. The user should note that the bridge filter will only examined frames from interfaces which is part of the bridge itself. Twenty filter rules are supported with bridge filtering.
The User Interface for Bridge Filter allows the user to add/edit/delete, as well as, enable the filter rules. To add a rules, simply define the source MAC address, destination MAC address and frame type with desired filtering type (i.e. allow/deny), and press the "Add" button. The MAC address must be in a xx-xx-xx-xx-xx-xx format, with 00-00-00-00-00-00 as "don't care". Blanks can be used in the MAC address space, and would be considered also as "don't care".
To edit/modify an exist filter rule, select the desired rule created previously from "Add" in the "Edit" select box. The selected filter rule will appear on top section, as with the "Add" filter rule. Make the desired change to the MAC address, frame type and/or access type, and press "Apply".
To delete filter rule(s), select the filter rule entry to delete in the "Delete" selection box. Note that multiple deletion is possible. Once all the desired filter rule(s) is/are selected for deletion, press the "Apply" button. The "Select All" select box can also be used to delete all the filter rule. It provides a quick method of selecting all filter rules for deletion.
The "Enable Bridge Filters" button allow the user to enable or disable bridge filtering. It can be set/unset during any add/edit/delete operation. It can also be set/unset independently by just pressing the "Apply" button.
Note: There are three hidden filter rules within the bridge filter table. These rules are entered automatically by the system to ensure the user does not "lock" themselves out of the system. The first rule allows any and all ARP frames through the system. The second rule allows all IPv4 frames with the destination MAC address of the bridge to go through. The third rule allows all IPv4 frames with the source MAC address of the bridge to go through.

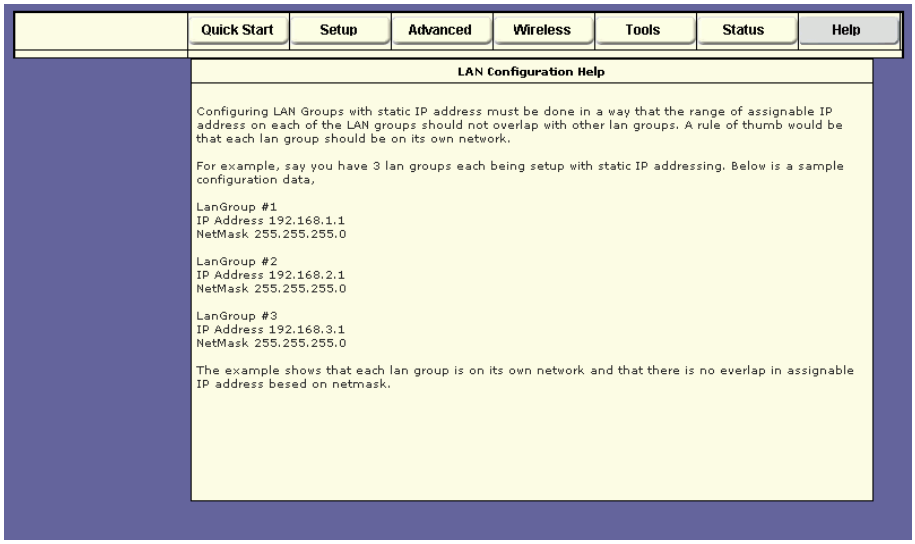
LAN Clients

Help section for LAN Clients.


Quick Start
Setup
Advanced
Wireless
Tools
Status
Help
LAN Clients Help
Using this feature user can see all the PCs on the LAN segment. Each PC is qualified to be either "dynamic" (PC obtained a lease from this router) or "static" (PC has a manually configured IP address).
User can add a "static" IP address(belonging to the network segment of the router LAN IP address). Any existing static entry falling within dhcp server's range can be deleted and the IP address would be made available for future allocation.
Once an IP address is allocated it shows up in the list of LAN clients as a "dynamic" entry. Any dynamic entry can be converted into static by using "reserve" checkbox.
Note: Dynamic clients show up in the list only when DHCP server is running.

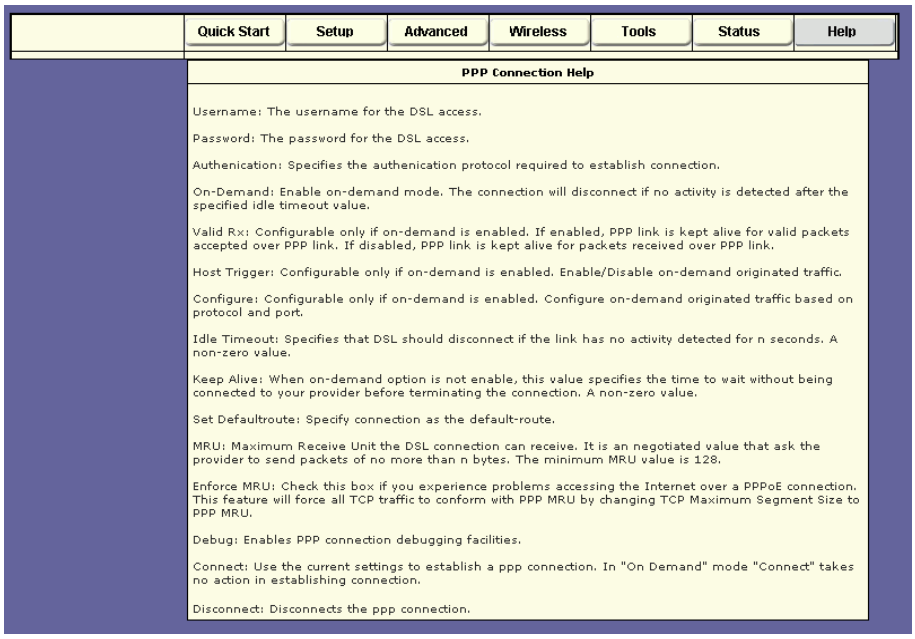
LAN Group Configuration

Help section for Configuring LAN Groups with static IP Address.


Quick Start
Setup
Advanced
Wireless
Tools
Status
Help
LAN Configuration Help
Configuring LAN Groups with static IP address must be done in a way that the range of assignable IP address on each of the LAN groups should not overlap with other lan groups. A rule of thumb would be that each lan group should be on its own network.
For example, say you have 3 lan groups each being setup with static IP addressing. Below is a sample configuration data,
LanGroup #1
IP Address 192.168.1.1
NetMask 255.255.255.0
LanGroup #2
IP Address 192.168.2.1
NetMask 255.255.255.0
LanGroup #3
IP Address 192.168.3.1
NetMask 255.255.255.0
The example shows that each lan group is on its own network and that there is no everlap in assignable IP address besed on netmask.

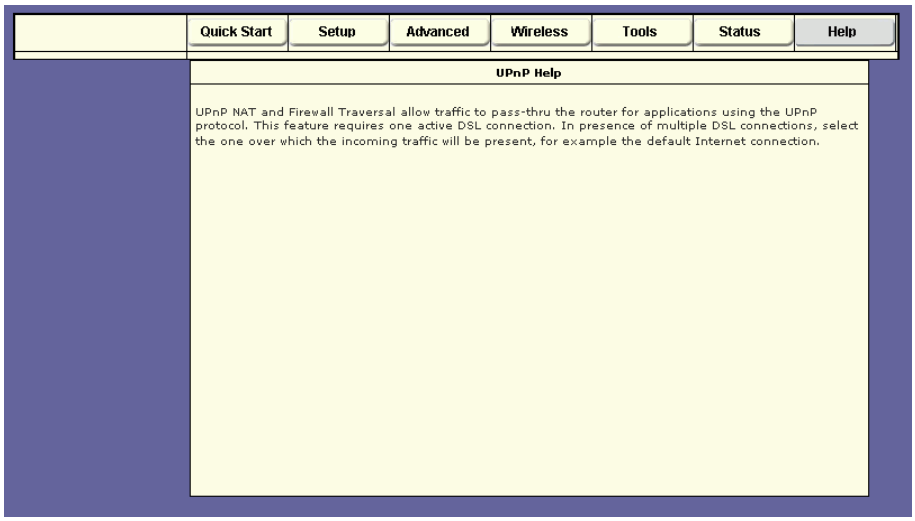
PPP Connection

Help for establishing a PPP Connection.


Quick Start
Setup
Advanced
Wireless
Tools
Status
Help
PPP Connection Help
Username: The username for the DSL access.
Password: The password for the DSL access.
Authenication: Specifies the authenication protocol required to establish connection.
On-Demand: Enable on-demand mode. The connection will disconnect if no activity is detected after the specified idle timeout value.
Valid Rx: Configurable only if on-demand is enabled. If enabled, PPP link is kept alive for valid packets accepted over PPP link. If disabled, PPP link is kept alive for packets received over PPP link.
Host Trigger: Configurable only if on-demand is enabled. Enable/Disable on-demand originated traffic.
Configure: Configurable only if on-demand is enabled. Configure on-demand originated traffic based on protocol and port.
Idle Timeout: Specifies that DSL should disconnect if the link has no activity detected for n seconds. A non-zero value.
Keep Alive: When on-demand option is not enable, this value specifies the time to wait without being connected to your provider before terminating the connection. A non-zero value.
Set Defaultroute: Specify connection as the default-route.
MRU: Maximum Receive Unit the DSL connection can receive. It is an negotiated value that ask the provider to send packets of no more than n bytes. The minimum MRU value is 128.
Enforce MRU: Check this box if you experience problems accessing the Internet over a PPPoE connection. This feature will force all TCP traffic to conform with PPP MRU by changing TCP Maximum Segment Size to PPP MRU.
Debug: Enables PPP connection debugging facilities.
Connect: Use the current settings to establish a ppp connection. In "On Demand" mode "Connect" takes no action in establishing connection.
Disconnect: Disconnects the ppp connection.

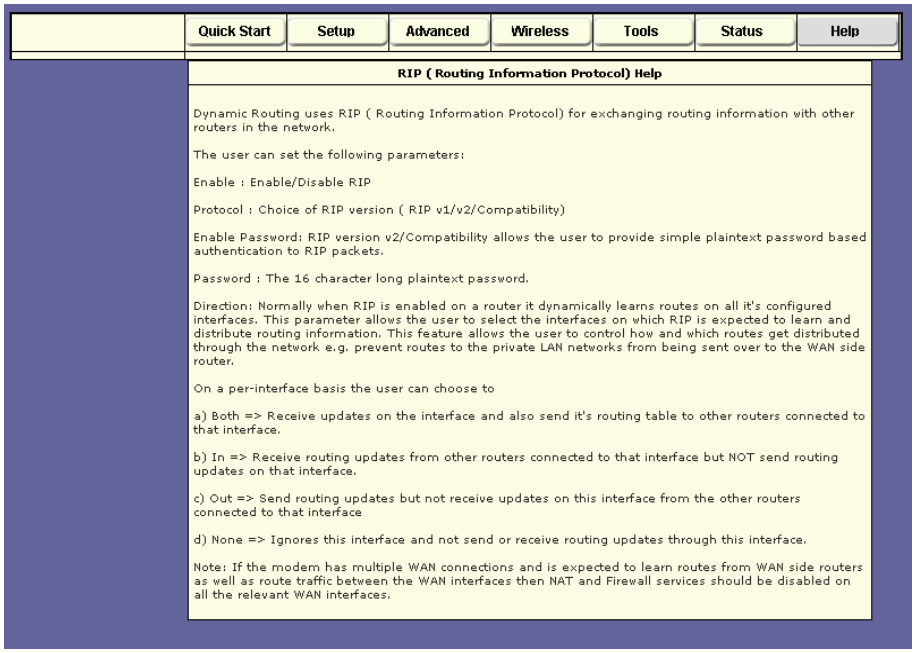
UPnP Help

Help pages for UPnP.


Quick Start
Setup
Advanced
Wireless
Tools
Status
Help
UPnP Help
UPnP NAT and Firewall Traversal allow traffic to pass-thru the router for applications using the UPnP protocol. This feature requires one active DSL connection. In presence of multiple DSL connections, select the one over which the incoming traffic will be present, for example the default Internet connection.

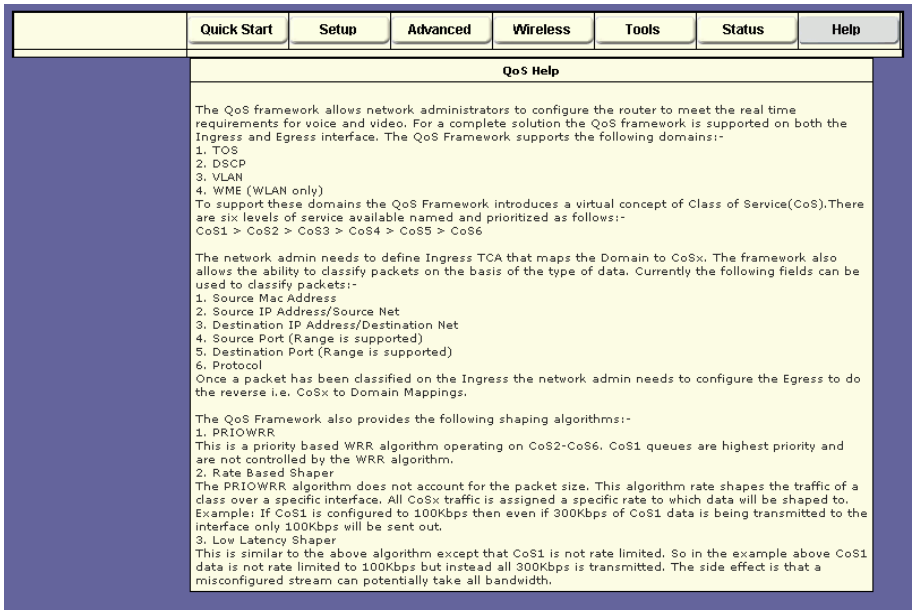
RIP Help

Help section for RIP (Routing Information Protocol).


Quick Start
Setup
Advanced
Wireless
Tools
Status
Help
RIP (Routing Information Protocol) Help
Dynamic Routing uses RIP (Routing Information Protocol) for exchanging routing information with other routers in the network.
The user can set the following parameters:
Enable : Enable/Disable RIP
Protocol : Choice of RIP version (RIP v1/v2/Compatibility)
Enable Password: RIP version v2/Compatibility allows the user to provide simple plaintext password based authentication to RIP packets.
Password : The 16 character long plaintext password.
Direction: Normally when RIP is enabled on a router it dynamically learns routes on all it's configured interfaces. This parameter allows the user to select the interfaces on which RIP is expected to learn and distribute routing information. This feature allows the user to control how and which routes get distributed through the network e.g. prevent routes to the private LAN networks from being sent over to the WAN side router.
On a per-interface basis the user can choose to
a) Both => Receive updates on the interface and also send it's routing table to other routers connected to that interface.
b) In => Receive routing updates from other routers connected to that interface but NOT send routing updates on that interface.
c) Out => Send routing updates but not receive updates on this interface from the other routers connected to that interface
d) None => Ignores this interface and not send or receive routing updates through this interface.
Note: If the modem has multiple WAN connections and is expected to learn routes from WAN side routers as well as route traffic between the WAN interfaces then NAT and Firewall services should be disabled on all the relevant WAN interfaces.

QoS Help

Help section for IP QoS.


Quick Start
Setup
Advanced
Wireless
Tools
Status
Help
QoS Help
The QoS framework allows network administrators to configure the router to meet the real time requirements for voice and video. For a complete solution the QoS framework is supported on both the Ingress and Egress interface. The QoS Framework supports the following domains:-
1. TOS
2. DSCP
3. VLAN
4. WME (WLAN only)
To support these domains the QoS Framework introduces a virtual concept of Class of Service(CoS).There are six levels of service available named and prioritized as follows:-
CoS1 > CoS2 > CoS3 > CoS4 > CoS5 > CoS6
The network admin needs to define Ingress TCA that maps the Domain to CoSx. The framework also allows the ability to classify packets on the basis of the type of data. Currently the following fields can be used to classify packets:-
1. Source Mac Address
2. Source IP Address/Source Net
3. Destination IP Address/Destination Net
4. Source Port (Range is supported)
5. Destination Port (Range is supported)
6. Protocol
Once a packet has been classified on the Ingress the network admin needs to configure the Egress to do the reverse i.e. CoSx to Domain Mappings.
The QoS Framework also provides the following shaping algorithms:-
1. PRIOWRR
This is a priority based WRR algorithm operating on CoS2-CoS6. CoS1 queues are highest priority and are not controlled by the WRR algorithm.
2. Rate Based Shaper
The PRIOWRR algorithm does not account for the packet size. This algorithm rate shapes the traffic of a class over a specific interface. All CoSx traffic is assigned a specific rate to which data will be shaped to. Example: If CoS1 is configured to 100Kbps then even if 300Kbps of CoS1 data is being transmitted to the interface only 100Kbps will be sent out.
3. Low Latency Shaper
This is similar to the above algorithm except that CoS1 is not rate limited. So in the example above CoS1 data is not rate limited to 100Kbps but instead all 300Kbps is transmitted. The side effect is that a misconfigured stream can potentially take all bandwidth.

Troubleshooting

This chapter gives information about troubleshooting your ADSL Router.
After each problem description, instructions are provided to help you diagnose and solve the problem.
For the common problems listed, go to the section indicated.

- Is the router on?
- Have I connected the router correctly?
  Go to Basic Functioning.

- I can't access the router's configuration with my browser.
  Go to Troubleshooting the Web Configuration Interface.

- I've configured the router but I can't access the Internet.
  Go to Troubleshooting the ISP Connection.

- I can't remember the router's configuration password.
- I want to clear the configuration and start over again.
  Go to **Restoring the Default Configuration and Password**.

Basic Functioning

After you turn on power to the router, the following sequence of events should occur:

1. When power is first applied, verify that the Power LED is on.
2. Verify that other LED lights within a few seconds, indicating that the self-test procedure is running.
3. After approximately 30 seconds, verify that :
   a. The LAN port LEDs are lit for any local ports that are connected.
   b. The WAN port LED is lit.

If a port's LED is lit, a link has been established to the connected device.
If any of these conditions does not occur, refer to the appropriate following section.

Power LED Not On

If the Power and other LEDs are off when your router is turned on :

- Make sure that the power cord is properly connected to your router and that the power supply adapter is properly connected to a functioning power outlet.
- Check that you are using the 12V AC/800mA power adapter supplied by ADSL for this product.
  If the error persists, you have a hardware problem and should contact technical support.

If all LEDs are still on one minute after power up:

- ❖ Cycle the power to see if the router recovers.
- ❖ Clear the router's configuration to factory defaults. This will set the router's IP address to **192.168.1.1**.

  If the error persists, you might have a hardware problem and should contact technical support.

LAN or WAN Port LEDs Not On

If either the LAN LEDs or WAN LED do not light when the Ethernet connection is made, check the following:

- ❖ Make sure that the Ethernet cable connections are secure at the router and at the hub or workstation.
- ❖ Make sure that power is turned on to the connected hub or workstation.
- ❖ Be sure you are using the correct cable :

  When connecting the router's WAN ADSL port, use the cable that was supplied with the ADSL.

Troubleshooting the Web Configuration Interface

If you are unable to access the router's Web Configuration interface from a computer on your local network, check the following:

- ❖ If you are using an Ethernet-connected computer, check the Ethernet connection between the computer and the router as described in the previous section.
- ❖ If your PC uses a Fixed (Static) IP address, ensure that it is using an IP Address within the range 192.168.1.2 to 192.168.1.254 and thus compatible with the ADSL Router default IP Address of 192.168.1.1. Also, the Network Mask should be set to 255.255.255.0 to match the ADSL Router. In Windows, you can check these settings by using Control Panel-Network to check the Properties for the TCP/IP protocol.

Follow the instructions to configure your computer.

Note: If your computer's IP address is shown as 169.254.x.x:

Recent versions of Windows and MacOS will generate and assign an IP address if the computer cannot reach a DHCP server.

These auto-generated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the computer to the router and reboot your computer.

- ❖ If your router's IP address was changed and you do not know the current IP address, clear the router's configuration to factory defaults. This will set the router's IP address to **192.168.1.1**.

Using the Reset button.

- Make sure your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click Refresh to be sure the Java applet is loaded.
- Try quitting the browser and launching it again.
- Make sure you are using the correct login information. The factory default login name is **Admin** and the password is **Admin**.

Make sure that CAPS LOCK is off when entering this information.

If the router does not save changes you have made in the Web Configuration Interface, check the following:

- When entering configuration settings, be sure to click the APPLY button before moving to another menu or tab, or your changes are lost.

Click the Refresh or Reload button in the Web browser. The changes may have occurred, but the Web browser may be caching the old configuration.

Troubleshooting the ISP Connection

If your router is unable to access the Internet, you should check the ADSL connection, then the WAN TCP/IP connection.

ADSL link

If your router is unable to access the Internet, you should first determine whether you have an ADSL link with the service provider.
The state of this connection is indicated with the WAN LED.

WAN LED On or Blinking

If your WAN LED is on or blinking, then you have a good ADSL connection.
You can be confident that the service provider has connected your line correctly and that your wiring is correct.

WAN LED Off

If your WAN LED is blinking, then your router is attempting to make an ADSL connection with the service provider. The LED should turn on within several minutes.
If the WAN LED does not turn on, disconnect all telephones on the line.
If this solves the problem, reconnect the telephones one at a time, being careful to use a splitter on each telephone.
If the splitters are connected correctly, you should be able to connect all your telephones.
If disconnecting telephones does not result in a green WAN LED, there may be a problem with your wiring.

If the telephone company has tested the ADSL signal at your Network Interface Device (NID), then you may have poor quality wiring in your house.

If disconnecting telephones does not result in a green WAN LED the problem may be one of the following:

- ❖ Check that the telephone company has made the connection to your line and tested it.
- ❖ Verify that you are connected to the correct telephone line. If you have more than one phone line, be sure that you are connected to the line with the ADSL service.

It may be necessary to use a swapper if you ADSL signal is on pins 1 and 4 or the RJ-11 jack. The ADSL Router uses pins 2 and 3.

Obtaining a WAN IP Address

If your router is unable to access the internet, and your WAN LED is on or blinking, you should determine whether the router is able to obtain a WAN IP address from the ISP.

Unless you have been assigned a static IP address, your router must request an IP address from the ISP.

You can determine whether the request was successful using the browser interface.

To check the WAN IP address from the browser interface:

1. Launch your browser and select an external site such as www.yahoo.com.
2. Access the Main Menu of the router's configuration at **http://192.168.1.1**.
3. Under the Maintenance heading check that an IP address is shown for the WAN Port.
   If 0.0.0.0 is shown, your router has not obtained an IP address from your ISP.

If your router is unable to obtain an IP address from the ISP, the problem may be one of the following:

- ❖ Your ISP may require a Multiplexing Method or **V**irtual **P**ath **I**dentifier/**V**irtual **C**hannel **I**dentifier (**VPI/VCI**) parameter.
  Verify with your ISP the Multiplexing Method and parameter value, and update the router's ADSL Settings accordingly.
- ❖ Your ISP may require a login program.
  Ask your ISP whether they require PPP over Ethernet (PPPoE) or PPP over ATM (PPPOA) login.
- ❖ If you have selected a login program, you may have incorrectly set the Service Name, User Name and Password. See "Troubleshooting PPPoE or PPPoA", below.
- ❖ Your ISP may check for your computer's host name.

Assign the computer Host Name of your ISP account to the router in the browser-based Setup Wizard.

- ❖ Your ISP only allows one Ethernet MAC address to connect to Internet, and may check for your computer's MAC address. In this case:
  Inform your ISP that you have bought a new network device, and ask them to use the router's MAC address.
  Or configure your router to spoof your computer's MAC address. This can be done in the Basic Settings menu.

Troubleshooting PPPoE or PPPoA

The PPPoE or PPPoA connection can be debugged as follows:

1. Access the Main Menu of the router at **http://192.168.1.1**.
2. Under the Maintenance heading, select the Router Status link.
3. Click the Connection Status button.
4. If all of the steps indicate "OK" then your PPPoE or PPPoA connection is up and working.
5. If any of the steps indicates "Failed", you can attempt to reconnect by clicking "Connect".
   The router will continue to attempt to connect indefinitely.

If you cannot connect after several minutes, you may be using an incorrect Service Name, User Name or Password. There also may be a provisioning problem with your ISP.

Note: Unless you connect manually, the router will not authenticate using PPPoE or PPPoA until data is transmitted to the network.

Troubleshooting Internet Browsing

If your router can obtain an IP address but your computer is unable to load any Web pages from the Internet:

- ❖ Your computer may not recognize any DNS server addresses.

A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses.
Typically your ISP will provide the addresses of one or two DNS servers for your use. If you entered a DNS address during the router's configuration, reboot your computer and verify the DNS address.
Alternatively, you can configure your computer manually with DNS addresses, as explained in your operating system documentation.

- ❖ Your computer may not have the router configured as its TCP/IP router.

If your computer obtains its information from the router by DHCP, reboot the computer

and verify the router address.

Troubleshooting a TCP/IP Network Using the Ping Utility

Most TCP/IP terminal devices and routers contain a ping utility that sends an echo request packet to the designated device. The device then responds with an echo reply.

Troubleshooting a TCP/IP network is made very easy by using the ping utility in your computer.

Testing the LAN Path to Your Router

You can ping the router from your computer to verify that the LAN path to your router is set up correctly.

To ping the router from a PC running Windows 98se or later:

1. From the Windows toolbar, click the Start button and select Run.
2. In the field provided, type Ping followed by the IP address of the router, as in this example: **ping 192.168.1.1**
3. Click OK.

You should see a message like this one:

Pinging <IP address> with 32 bytes of data

If the path is working, you see this message:

Reply from < IP address >: bytes=32 time=NN ms TTL=xxx

If the path is not working, you see this message:

Request timed out

If the path is not functioning correctly, you could have one of the following problems:

Wrong physical connections

- Make sure the LAN port LED is on. If the LED is off, follow the instructions in "LAN or WAN Port LEDs Not On".
- Check that the corresponding LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and router.

❖ Wrong network configuration

- Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your PC or workstation.
- Verify that the IP address for your router and your workstation are correct and that the addresses are on the same subnet.

Testing the Path from Your Computer to a Remote Device

After verifying that the LAN path works correctly, test the path from your PC to a remote device.

From the Windows run menu, type:

ping -n 10 ***<IP address>***

where ***<IP address>*** is the IP address of a remote device such as your ISP's DNS server.

If the path is functioning correctly, replies as in the previous section are displayed.

If you do not receive replies:

- Check that your PC has the IP address of your router listed as the default router. If the IP configuration of your PC is assigned by DHCP, this information will not be visible in your PC's Network Control Panel. Verify that the IP address of the router is listed as the default router.
- Check to see that the network address of your PC (the portion of the IP address specified by the netmask) is different from the network address of the remote device.
- Check that your modem is connected and functioning.
- If your ISP assigned a host name to your PC, enter that host name as the Account Name in the Basic Settings menu.
- Your ISP could be rejecting the Ethernet MAC addresses of all but one of your PCs.

  Many broadband ISPs restrict access by only allowing traffic from the MAC address of your broadband modem, but some ISPs additionally restrict access to the MAC address of a single PC connected to that modem.

  If this is the case, you must configure your router to "clone" or "spoof" the MAC address from the authorized PC.

Restoring the Default Configuration and Password

This section explains how to restore the factory default configuration settings, changing the router's administration password to password and the IP address to **192.168.1.1**.

You can erase the current configuration and restore factory defaults in two ways:

- In Tools-> System Commands -> **Restore Defaults**.
- Use the Default Reset button on the rear panel of the router. Use this method for cases when the administration password or IP address is not known.

Using the Reset button

To restore the factory default configuration settings without knowing the administration password or IP address, you must use the Default Reset button on the rear panel of the router.

1. Press and hold the Default Reset button until all LED turns off (about 6 seconds).
2. Release the Default Reset button and wait for the router to reboot.

Appendix

Country	ISP	PVC
Australia	All Internet providers	VPI:8
		VCI:35
Belgium		VPI:0
		VCI:33
Canada	Telus	VPI:0
		VCI:35
Danmark	Cybercity	VPI:8
		VCI:35
	Tiscali	VPI:8
		VCI:35
Deutschland	1 & 1 Internet DSL	VPI:1
		VCI:32
	AOL DSL	VPI:1
		VCI:32
	Arcor DSL	VPI:8
		VCI:35
	Freenet DSL	VPI:1
		VCI:32
	Fireline networks	VPI:1
		VCI:32
	GMX Internet	VPI:1
		VCI:32
	Hansenet	VPI:8
		VCI:35
	Netcologne	VPI:8
		VCI:35
	Schlund	VPI:1
		VCI:35
	Snafu ADSL	VPI:1
		VCI:32
	Tiscali	VPI:1
		VCI:32
	T-online	VPI:1
		VCI:32
	Anderer Anbieter	VPI:1
		VCI:32
France	Wannadoo	VPI:8
		VCI:35
	Tiscali	VPI:8
		VCI:35

Country	ISP	PVC
ISRAEL	KPN PPPoE LLC	VPI:8
		VCI:48
Italian	Telecom Italia	VPI:8
		VCI:35
	Rest oil presente	VPI:8
		VCI:35
Netherlands	KPN PPPoA VC-MuX	VPI:8
		VCI:48
	BBeyond Bridge LLC	VPI:0
		VCI:33
	BBeyond PPPoA VC-MuX	VPI:0
		VCI:35
New Zealand	New Zealand Telecom	VPI:0
		VCI:100
Portugal	Todos os apresentador	VPI:0
		VCI:35
Spanish	Albura	VPI:1
		VCI:32
	Colt Teeccom	VPI:0
		VCI:35
	Earth	VPI:8
		VCI:32
Spanish	Eresmas	VPI:8
		VCI:35
	Jazztel	VPI:8
		VCI:35
	Ola Internet	VPI:8
		VCI:35
	Retevision	VPI:0
		VCI:35
	Terra	VPI:8
		VCI:32
	Tiscali	VPI:1
		VCI:32
	Telefornica	VPI:8
		VCI:32
	Telepac	VPI:8
		VCI:35
	Uni2	VPI:1
		VCI:33
	Ya.com	VPI:8
		VCI:32
	Wanadoo	VPI:8
		VCI:32
Suomi	Island ssimi	VPI:0
		VCI:35
	Landssimi	VPI:8
		VCI:48
	Vortex	VPI:8
		VCI:48

Country	ISP	PVC
Switserland	Alle anbieter	VPI:1
		VCI:32
Sverige	Skanova	VPI:8
		VCI:35
Taiwan	Hinet	VPI:0
		VCI:33
	Seednet	VPI:0
		VCI:33
United Arab Emirates	Etisalat Classical IP Single User	VPI:8
		VCI:35
	Etisalat Classical IP for Business	VPI:8
		VCI:35
United Kingdom	British Telecom	VPI:0
		VCI:38